Prisma® SD-WAN

Prisma SD-WAN – Zscaler Internet Access CloudBlade Deployment Guide

Release Number 1.4.1

Prisma SD-WAN Customer Support

For technical issues, contact Prisma SD-WAN Customer Support.

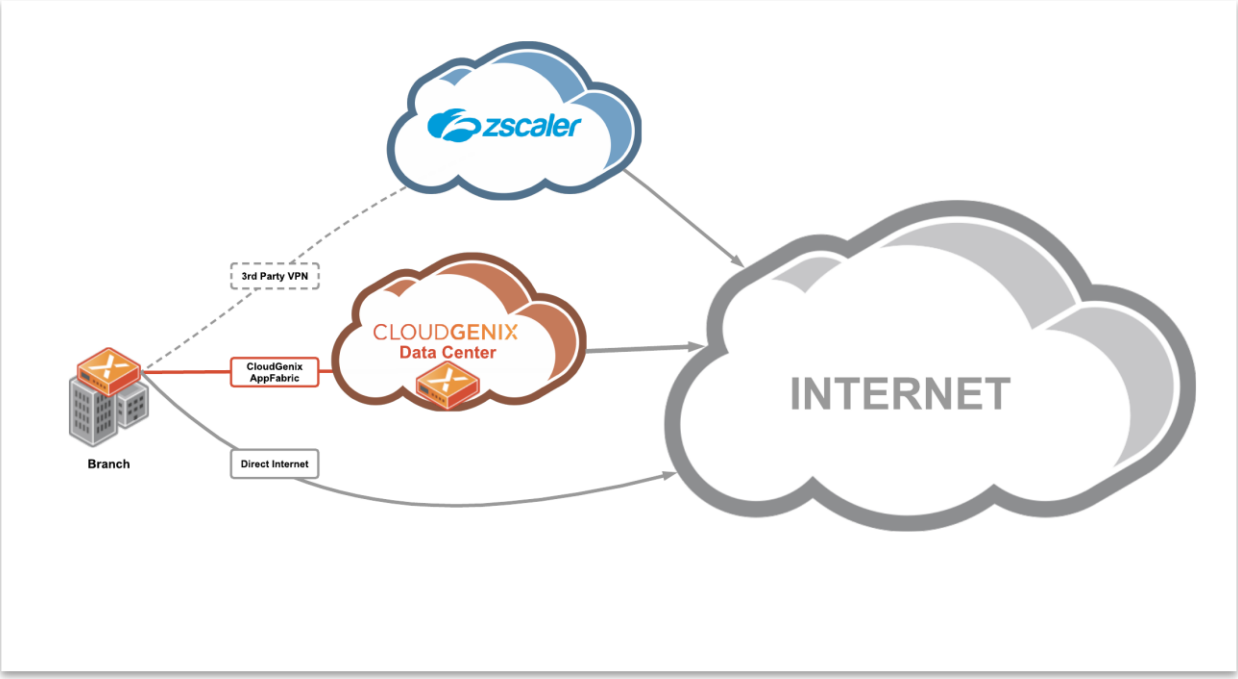
PHONE: 1-844-800-2469, Ext. 2
EMAIL: support@Prisma SD-WAN.com

Integrating with Zscaler Internet Access

As enterprises rely on SaaS or Cloud-based delivery models for business-critical applications, there is a compelling need for per-application policy enforcement without increasing remote office infrastructure. Traditional hardware-router based approaches are limited by heavy-handed 'all or nothing' policies for direct-to-internet versus policy enforcement per-application. Additionally, because router-based approaches are packet-based versus application-session based, they fail to meet application session-symmetry requirements, causing network and security outages.

The integration of Prisma SD-WAN SD-WAN and Zscaler Internet Access (ZIA), allows customers to have a lightweight remote office hardware footprint, while still being able to provide a full suite of application-specific security policies.

To facilitate this integration, Prisma SD-WAN Release 5.1.1 and later provide CloudBlades to automatically integrate the Prisma SD-WAN Controller, Remote Prisma SD-WAN ION devices and Zscaler Enforcement Nodes (ZENs).



Note: The images in this document may have references to **CloudGenix** and the term **3rd Party** / **3rd Party VPN**. The CloudGenix instances now display as **Prisma SD-WAN**, and the new term for 3rd Party / 3rd Party VPN is **Standard VPN** on the Prisma SD-WAN web interface.

Prerequisites

The following items are required for configuring Prisma SD-WAN and Zscaler Internet Access integration:

Prisma SD-WAN

- An active Prisma SD-WAN subscription.
- Prisma SD-WAN AppFabric deployed at one or more locations.
- Physical and/or virtual ION devices running Release 5.1.9 or later.

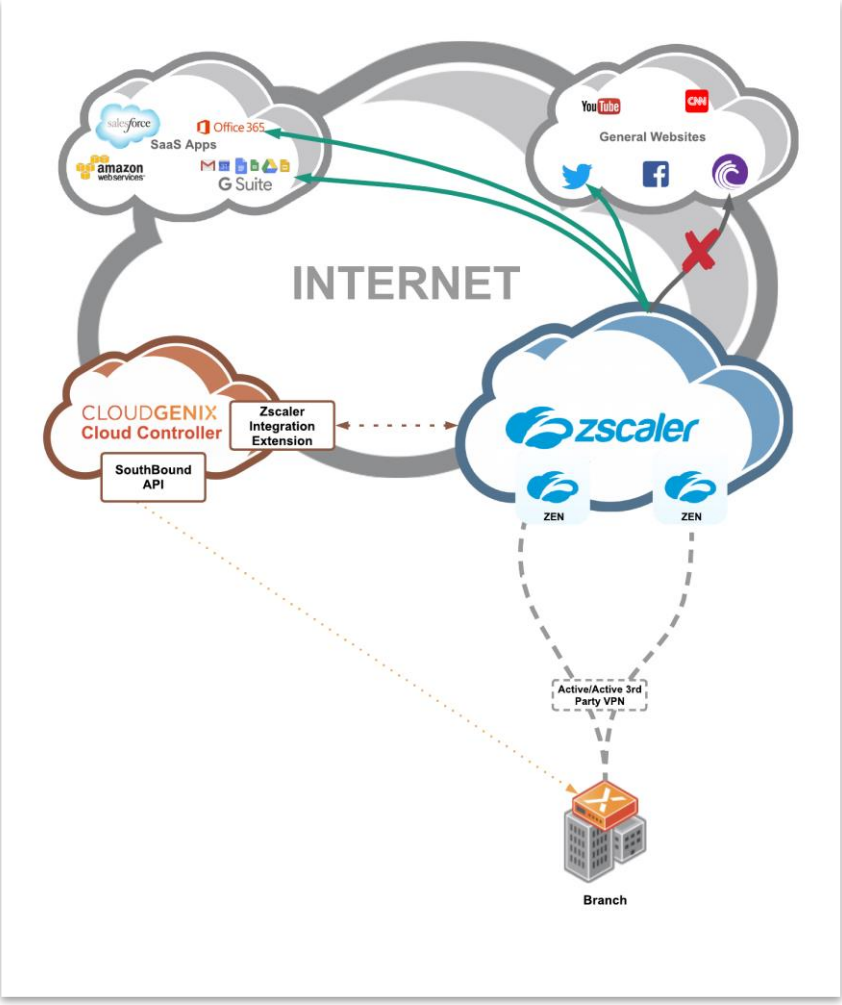
Zscaler

- An active Zscaler Internet Access Instance (in any cloud)
- Administrator login credentials for this instance.
- A partner administrator account and partner key

Plan the Deployment

The primary way to architecturally accomplish the Prisma SD-WAN and Zscaler Internet Access integration is via IPsec Standard VPNs from remote ION device endpoints to Zscaler. The Zscaler Integration CloudBlade provides the automatic creation, management, and maintenance of the IPsec Standard VPN tunnels by simply entering 'tags' on the appropriate Prisma SD-WAN objects.

To facilitate this tag-based configuration, the Prisma SD-WAN Portal must be configured and linked to Zscaler via a partner administrator account and an SD-WAN partner key.



Use the following steps to complete the integration:

Steps	Action
Step 1	Create a partner administrator role, create a partner administrator account and assign the role, and generate an SD-WAN partner key from the Zscaler portal.
Step 2	Configure and install the Zscaler CloudBlade in the Prisma SD-WAN Portal.
Step 3	Assign tags to objects in the Prisma SD-WAN Portal to automatically integrate those objects to Zscaler.
Step 4	Edit application network policy rules to send traffic to the Zscaler.

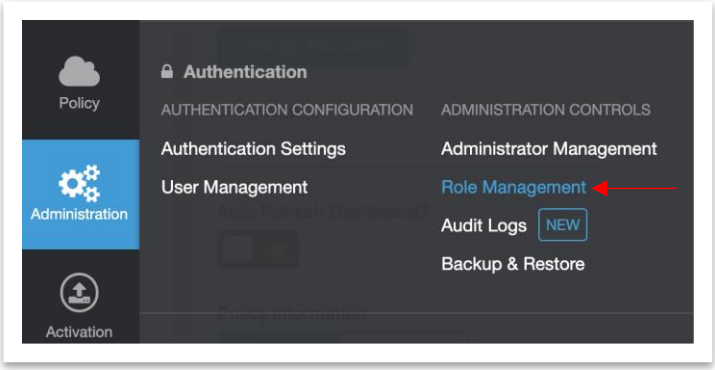
Note: Prior to configuring the Zscaler CloudBlade in the Prisma SD-WAN portal, make sure that the user account you are logged in with has **IP session lock disabled**. For more information, refer to *Improper Settings for Prisma SD-WAN User Doing Initial Installation*.

Acquire the Zscaler Information

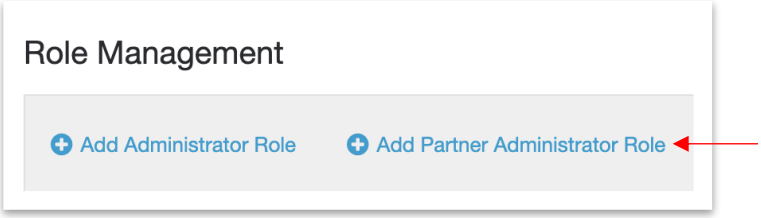
Before configuring Prisma SD-WAN to integrate with Zscaler, perform the following steps:

1. Create a partner administrator role with full access controls for **Locations** and **VPN Credentials** as follows:

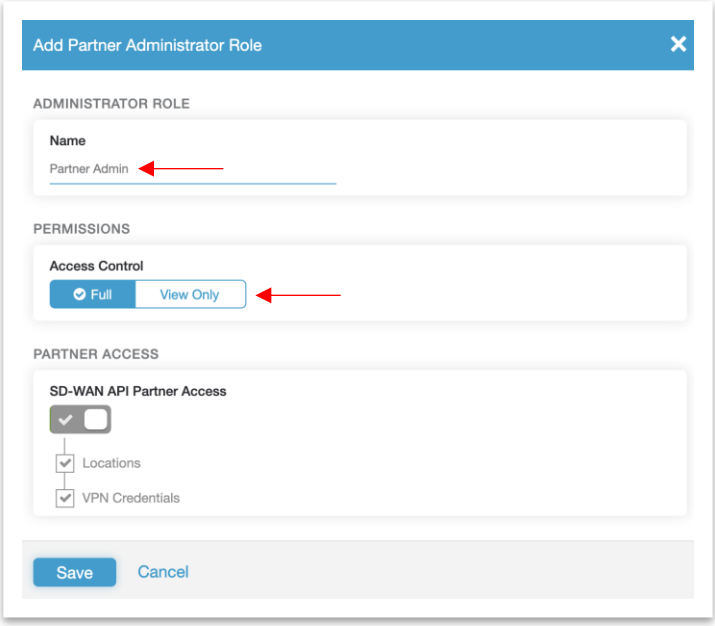
   a) From **Administration**, click **Role Management**.



   b) Click **Add Partner Administrator Role**.

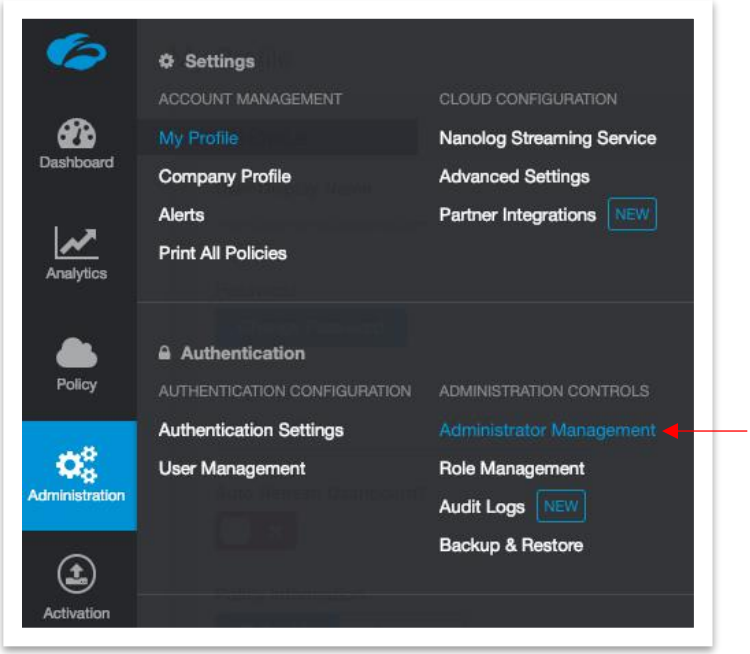


   c) On the **Add Partner Administrator Role** screen, select **Full** for **Access Control**. In the **Partner Access** section, select the **Locations** and **VPN Credentials** check boxes and click **Save**.

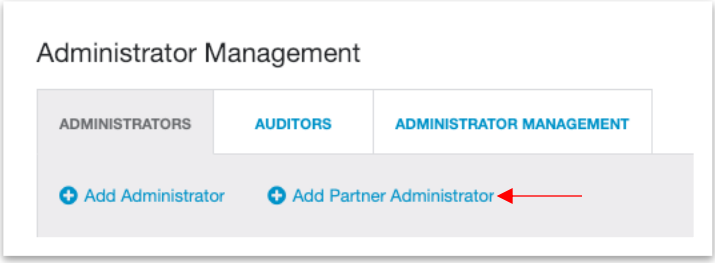


2. Create a **partner administrator account** and assign the **Partner Admin** role created in Step 1 as follows:

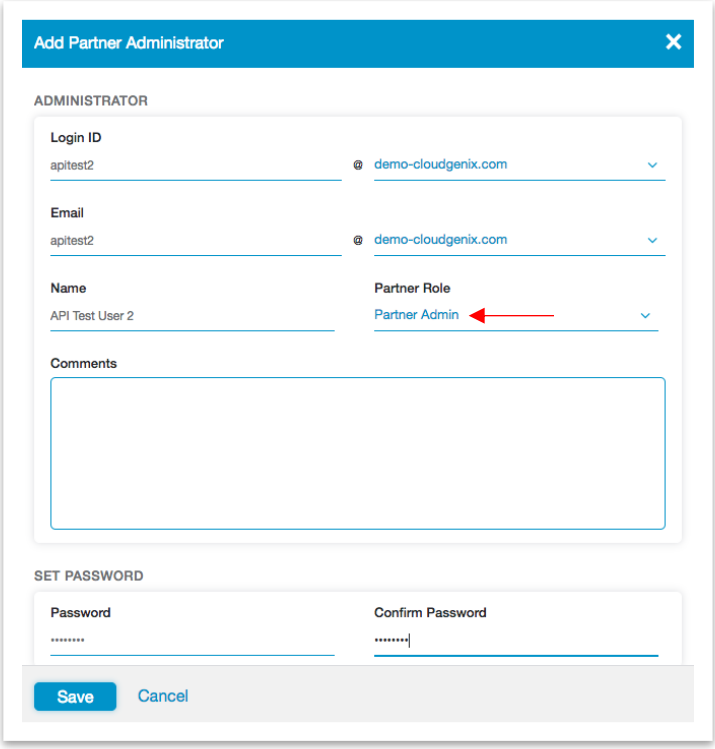
   a) From **Administration**, select **Administrator Management**.



   b) On the **Administrator Management** screen, click **Add Partner Administrator**.

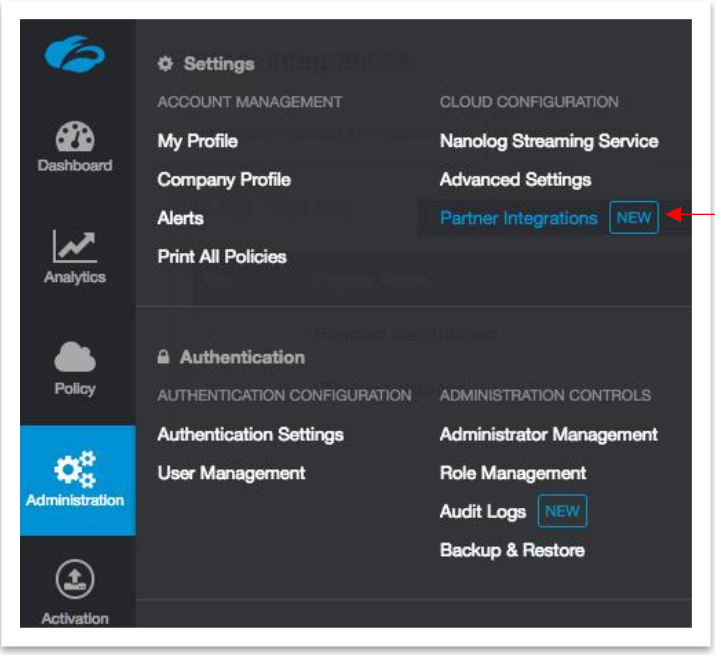


c) Select **Partner Admin** as the **Partner Role** and click **Save**.

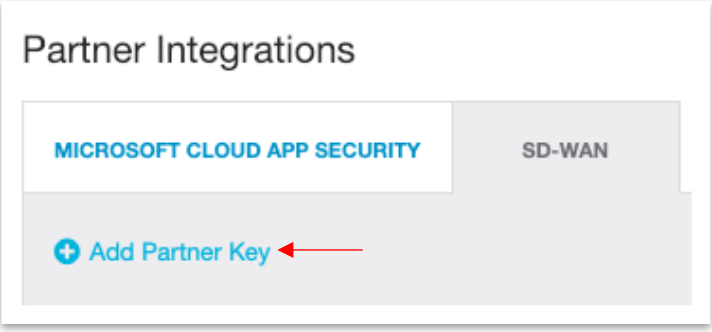


3. Generate an SD-WAN partner Key as follows:

   a) From **Administration**, select **Partner Integrations**.

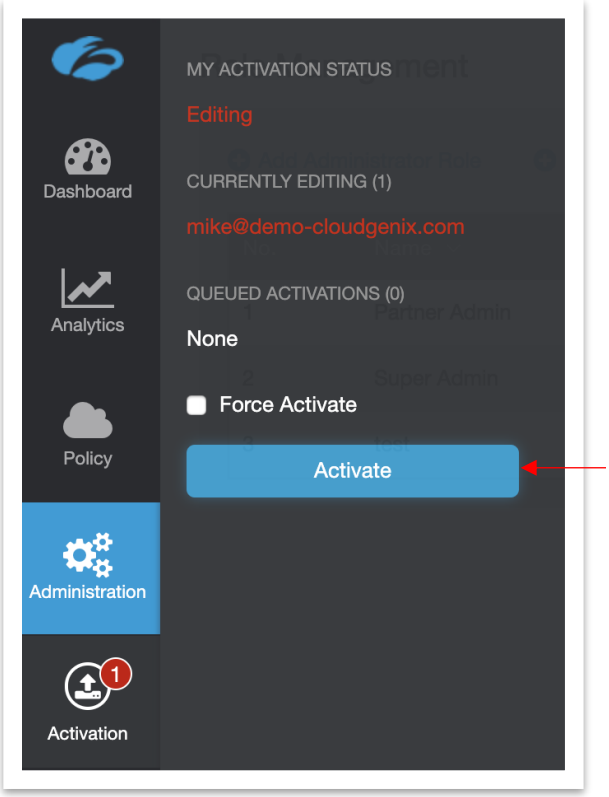


   b) On the **SD-WAN** tab, click **Add Partner Key**.



   c) The value of the key is displayed in the **Key** field. Copy this key, it will be needed during the configuration process.

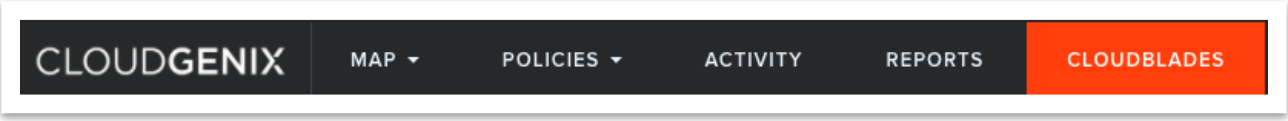
4. Activate pending changes on Zscaler by navigating to the **Activation** screen and clicking **Activate**.



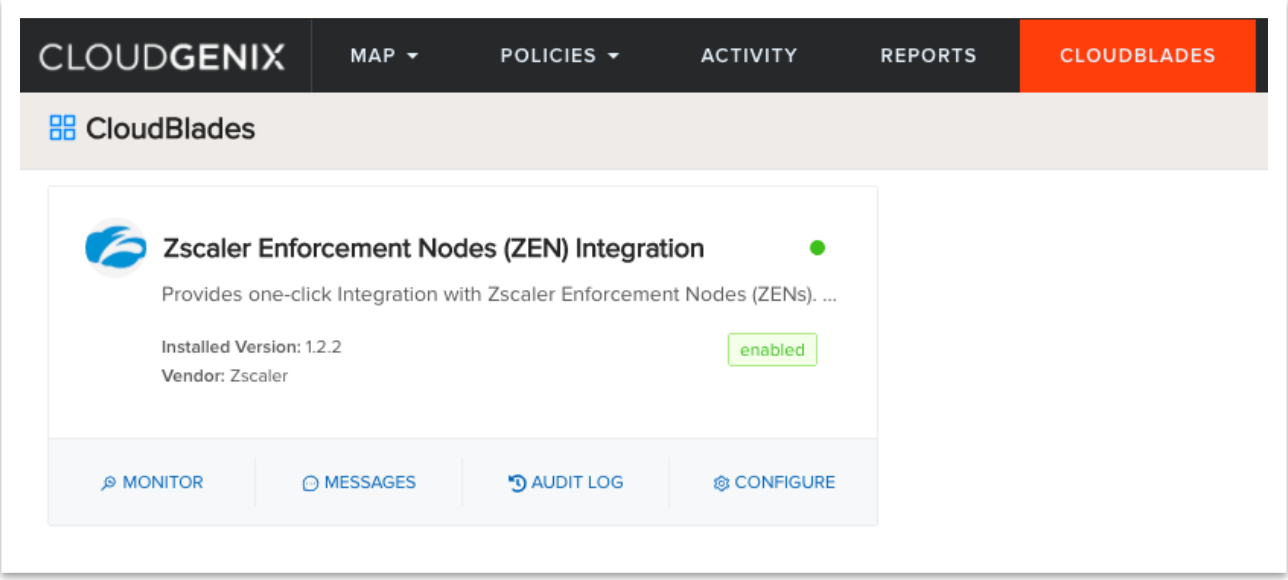
Configure and Install the Zscaler Integration CloudBlade

Next, configure the Prisma SD-WAN CloudBlade to prepare the Prisma SD-WAN Controller for integration.

1. From the Prisma SD-WAN Portal, click the **CloudBlades** tab.



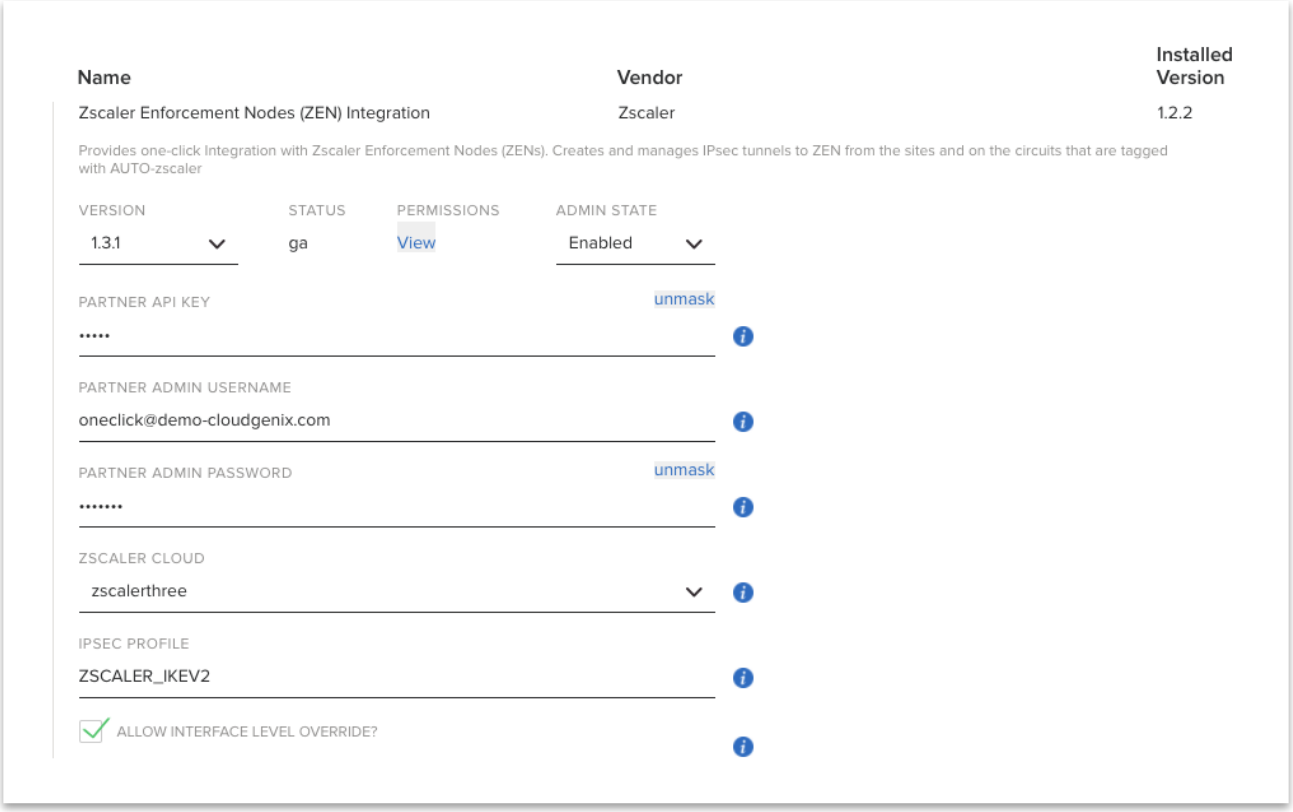
2. In **CloudBlades**, locate the **Zscaler Enforcement Nodes (ZEN) Integration CloudBlade**. If this CloudBlade does not appear, please contact Prisma SD-WAN Support.



3. Click **Configure** on the CloudBlade card to display the installation page. Enter the following information:
   a. From the **Version** drop-down list, select the required version.
   b. For **Admin State**, retain **Enabled**, which is the default value.
   c. For **API Key**, provide the SD-WAN key generated in the previous section.
   d. For **Partner Admin Username** and **Partner Admin Password,** provide the partner administrator account details created in the previous section.
   e. For **Zscaler cloud,** select the Zscaler cloud to which your subscription is attached (*zscalerthree* in the example below).

f. **Optionally**, specify the IPsec Profile name (case sensitive). The default is *ZSCALER_IKEV2*, which should be pre-provisioned along with the CloudBlade allocation. If this does not display, please contact Prisma SD-WAN Support.
g. If you select **Allow Interface Level Override** for the IPsec profile, it will allow administrators to change the IPsec profile referenced at the Standard VPN tunnel level without the CloudBlade overriding this change. This is typically useful in case of troubleshooting scenarios.
h. Optionally, provide the **base URL**. If left blank, the base URL will be derived from the *admin username* domain.

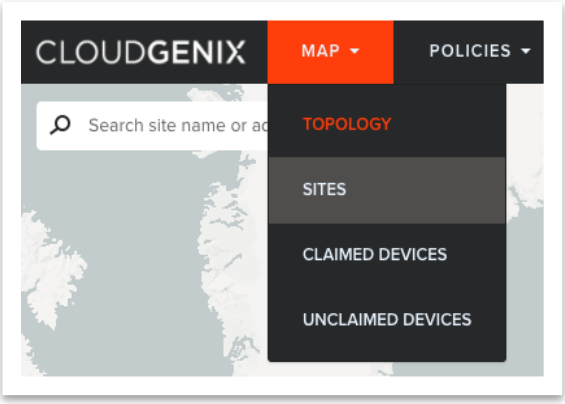
4. Once the settings have been configured, press the **Install** button (or **Save,** if the CloudBlade was previously installed).



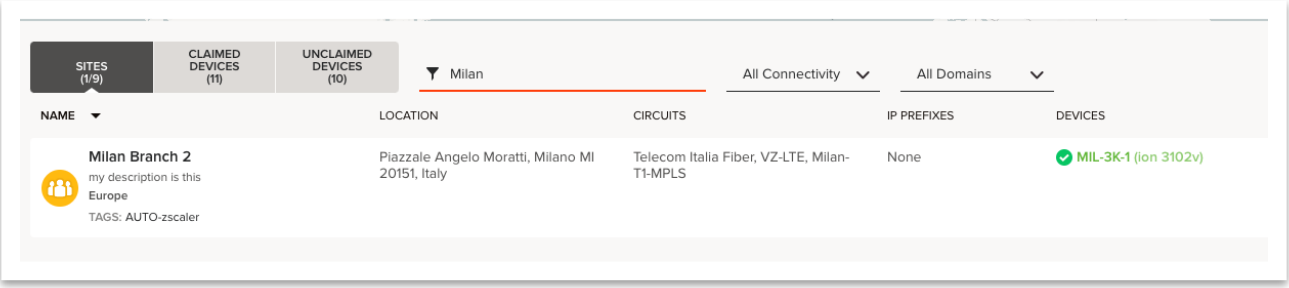
Assign Tags to Objects in the Prisma SD-WAN Portal

Once the CloudBlade is configured, the next task is to tag Prisma SD-WAN sites and circuit categories to denote which sites and circuit types are candidates for auto Standard VPN tunnel creation to Zscaler.

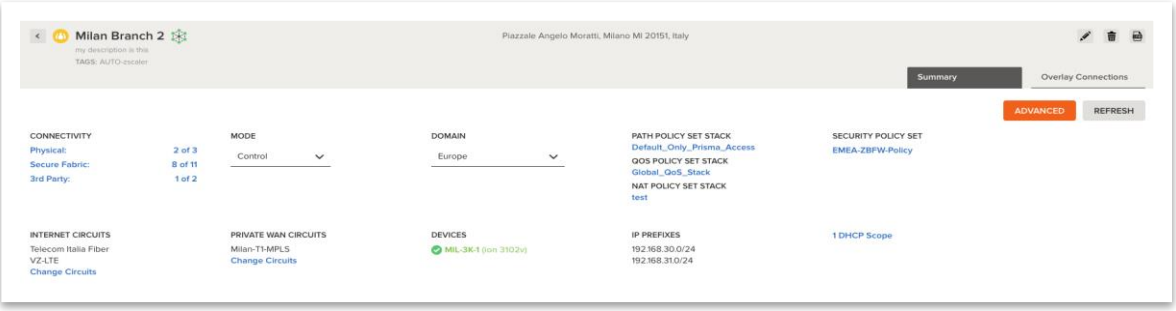
1. From the Prisma SD-WAN Portal, click **Map -> Sites**.



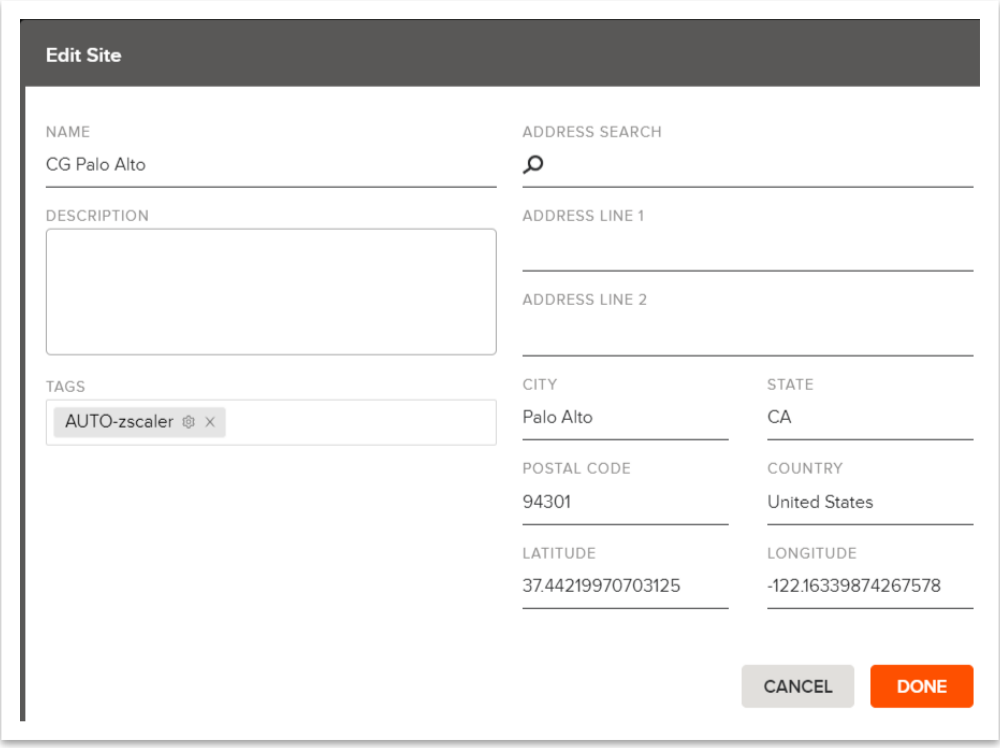
2. Search for a site to connect to Zscaler. Click on the site to bring up the site details.



3. On the top right of the site details screen, click the Edit (✎) icon.



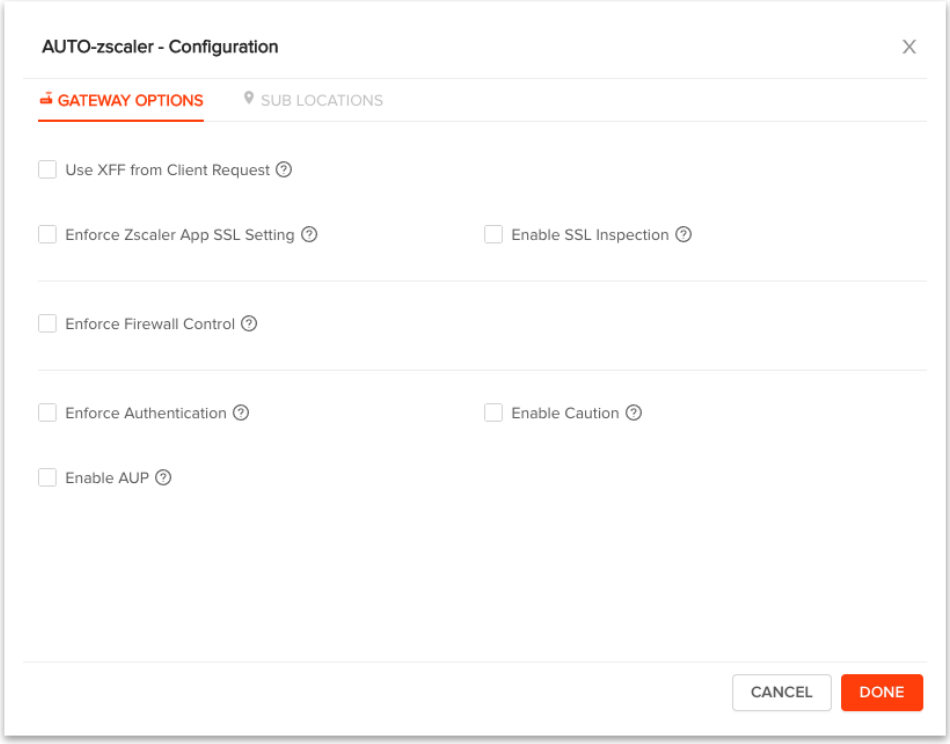
4. On the **Edit Site** screen, in the **TAGS** field, type **AUTO-zscaler** (case sensitive).



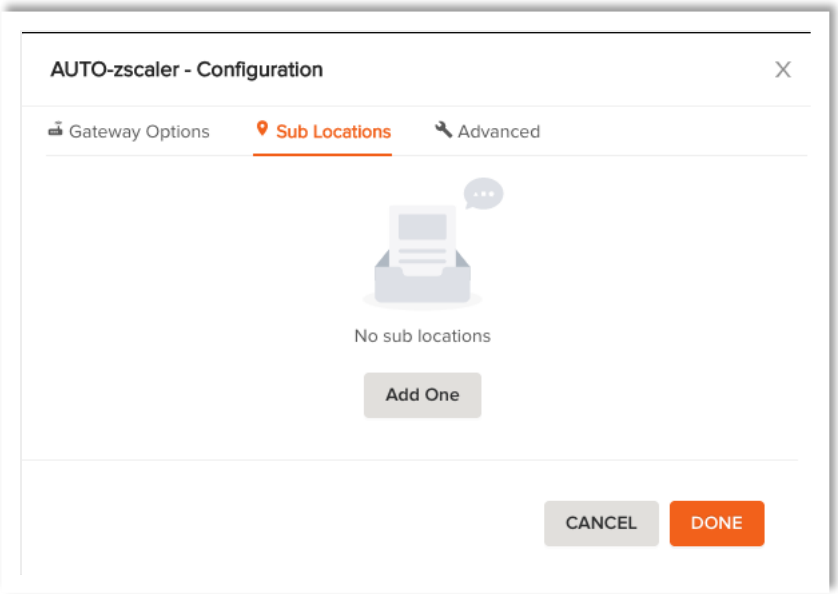
Note that this is a special tag as denoted by the **gear** icon.

5. **Optionally**, select the gear icon to configure the gateway options as required by your security team.

   a. If configuring gateway options only at the parent location level, specify the options as needed. This implies that all traffic from this location will be subject to the options configured here.
   Note: The gateway options, **Enforce Zscaler App SSL Setting** and **Enable SSL Inspection** shown in the image below are currently deprecated by Zscaler.

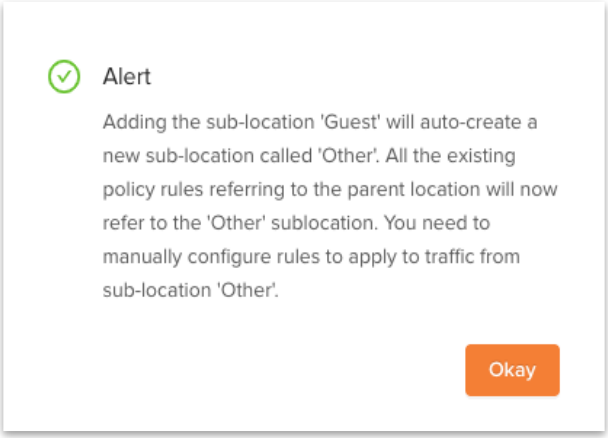


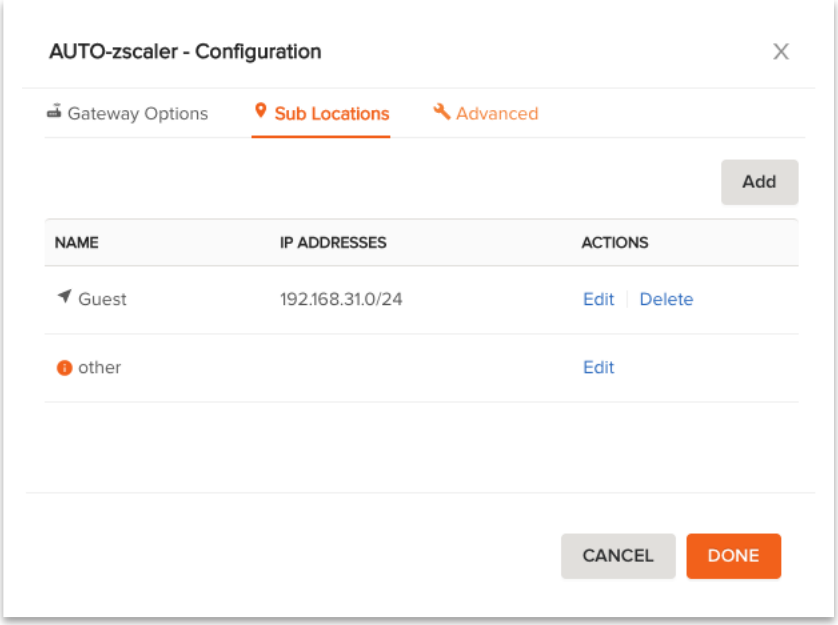
b. If you need to configure different gateway option settings for different sources of traffic from this site, then specify the appropriate sub location definition and settings from the **Sub Locations** tab.



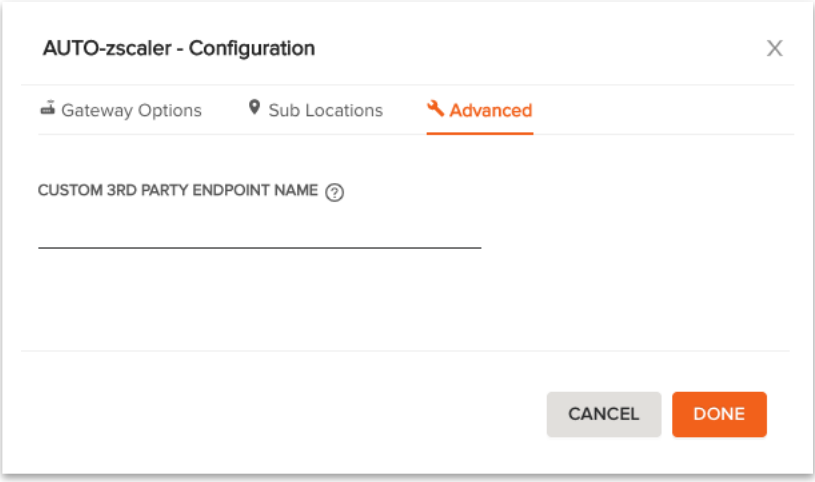
Note: In the **Sub Locations** tab, options **Enforce Zscaler App SSL Setting** and **Enable SSL Inspection** are currently deprecated and the option **Use XFF from Client Request** is disabled.

c. If you create a sub-location, make sure to specify the gateway options for the **other** location.





d. If there is a requirement to use a custom Standard VPN endpoint instead of the one which the CloudBlade manages and maintains, specify the endpoint under the **Advanced** tab.



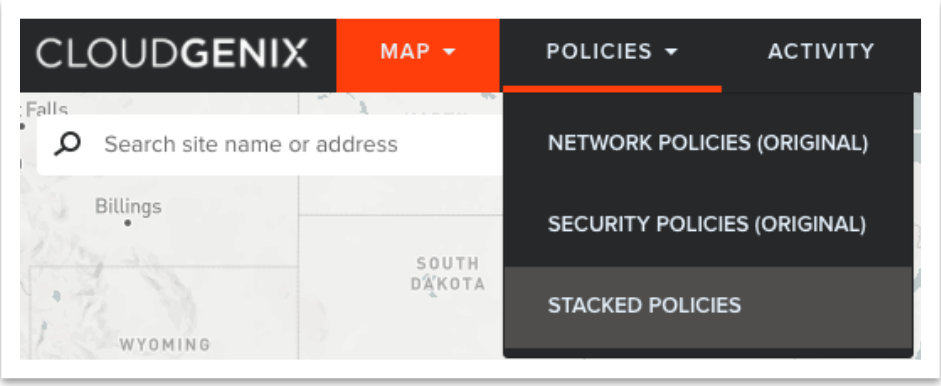
Note: The Standard VPN endpoint name is case sensitive and must be previously configured under **Stacked Policies -> Service & DC Groups -> Endpoints -> Standard VPN**

6. Click **Done**.

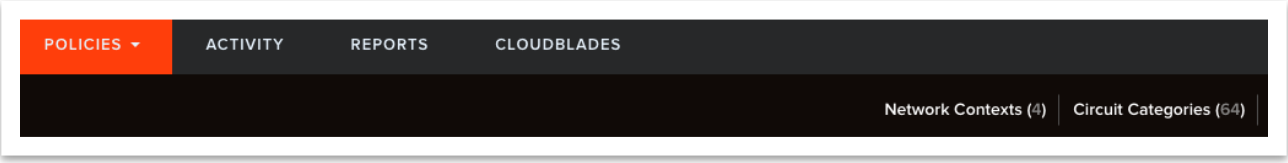
Now that the site has been tagged as enabled for Zscaler, we need to tag the circuit categories that can be used to establish a Standard VPN tunnel to Zscaler.

Note: This capability is useful if you want only specific types of circuits to be used for Zscaler integration or explicitly exclude certain circuit types. For example, a customer may not want to use their metered LTE circuit for Standard VPN establishment.

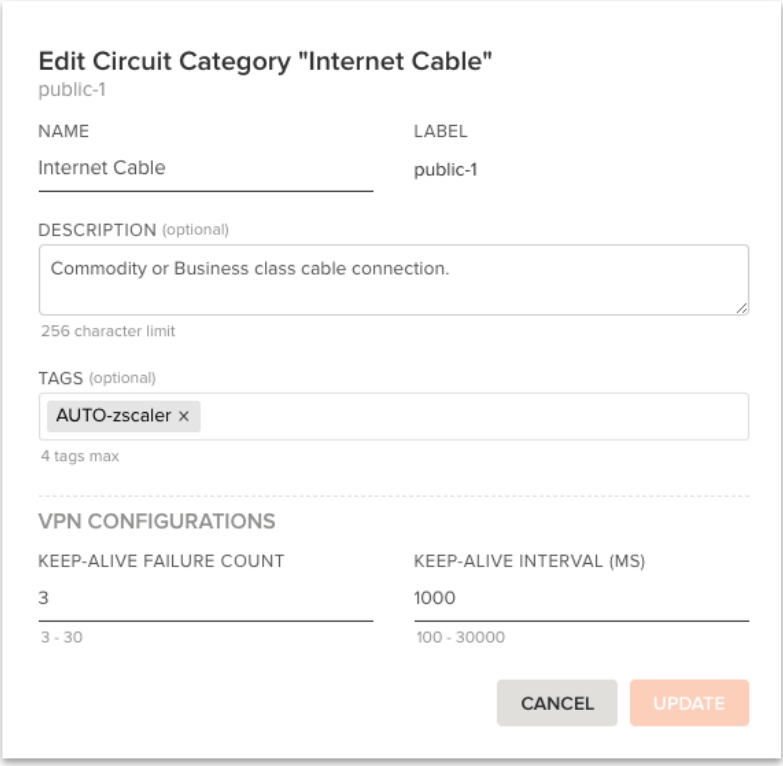
1. From the Prisma SD-WAN Portal, click **Policies > Stacked Policies.**



2. Click **Circuit Categories**.



3. Find the circuit categories that are associated with your site(s) from which you want the system to automatically build Standard VPN tunnels. Edit the circuit category, and enter **AUTO-zscaler** (case sensitive) in the **Tags** field.

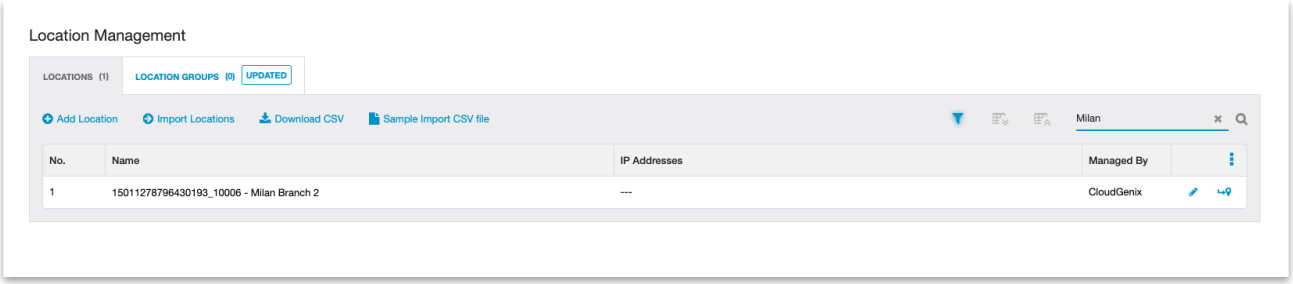


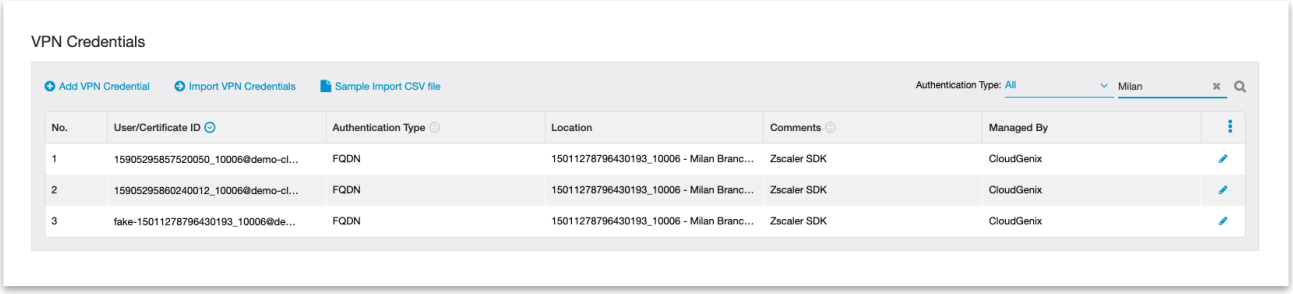
4. Click **Save**.

Once this configuration is completed, Standard VPN IPsec tunnels connecting the Prisma SD-WAN ION device and Zscaler will begin the creation/onboarding process in the next integration cycle (60 seconds). It may take several integration cycles for the tunnels to appear and be active on the Prisma SD-WAN portal.

Validate the Zscaler Configuration

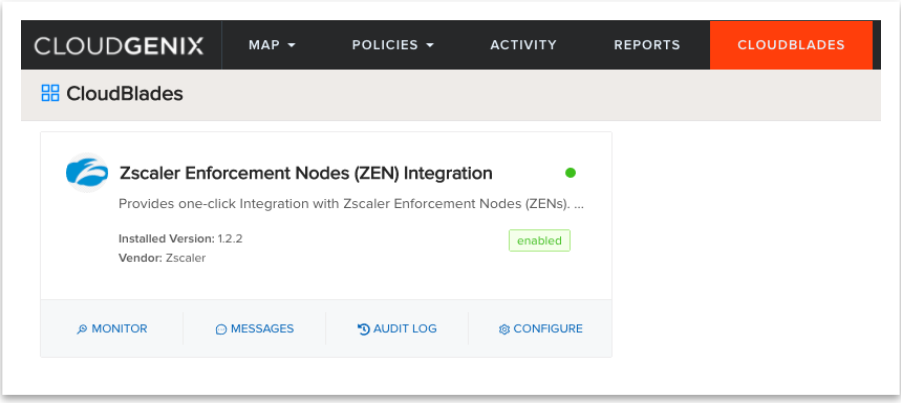
The Zscaler CloudBlade will provision **Locations** and unique **VPN Credentials** per tunnel within Zscaler. Below is a sample output of the deployment for the Milan Branch 2 site from the Zscaler portal. This site has two circuits. Note that there is a 3rd “fake” VPN credential which is never used, but is part of the initial location creation and onboarding process.



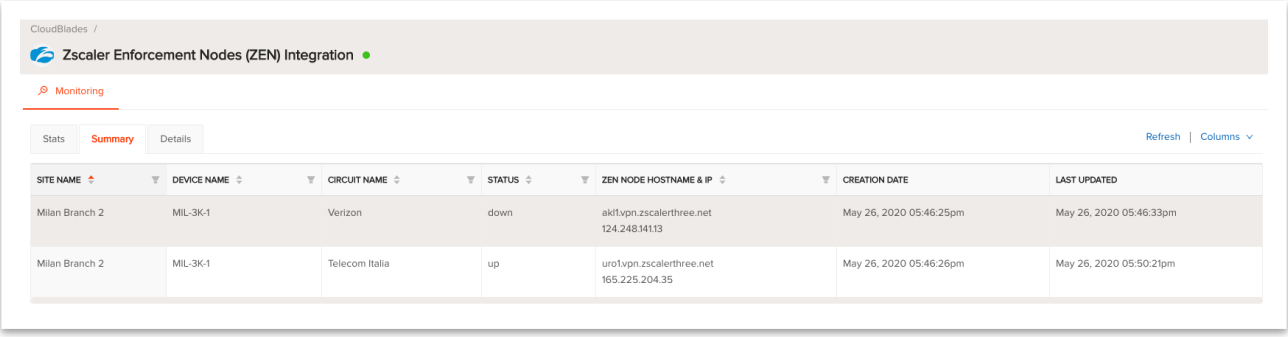


Starting with Zscaler CoudBlade version 1.2.2, the status of the deployment and tunnels can be validated on the **CloudBlades** page as follows:

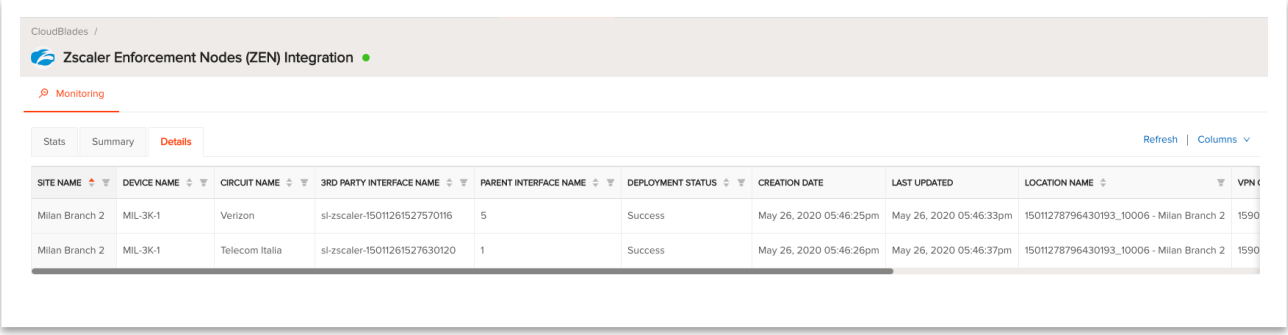
1. On the **CloudBlades** screen, click **Monitor**.



2. Select the **Summary** tab to see an overview of all the connected sites and ZEN node endpoints.



3. Select the **Details** tab to view the deployment status and the configuration details. These details are helpful for troubleshooting.



Edit Application Network Policy Rules

Once the CloudBlade configures the appropriate Standard VPN objects within Prisma SD-WAN and Zscaler, the administrator can reference the path (**Standard VPN**) and service group **(Zscaler**) within application network policies. The ION devices will make intelligent per-app path selections using the network policies to chain multiple path options together in Active-Active and Active-Backup modes.

Example:

- **Application A:** Take **Standard VPN** direct to Zscaler.
- **Application B**: Take **Standard VPN** direct to Zscaler; Backup to **Direct Internet**.
- **Application C**: Go to Internet via **Prisma SD-WAN Data Center**; Backup to **Standard VPN** direct to Zscaler.
- **Application D**: Use only **Direct Internet.**

The Prisma SD-WAN Secure Application Fabric (AppFabric) enables granular controls for virtually unlimited number of policy permutations down to the sub-application level. Here are some of the most common examples of how traffic policy can be configured per application:

- Send all internet-bound traffic from a set of branches to a Zscaler datacenter. (**Blanket Greylist**)
- Send all internet-bound traffic from a set of branches to a Zscaler datacenter with the exception of specific known applications. (**Greylist-Whitelist**)
- Send all internet traffic direct to the internet except for certain applications needing additional inspection or security. (**Whitelist-Greylist**)

In order to modify application policy, perform the steps below which are detailed in the following sections:

1. Understand Service and Data Center Groups
2. Verify Standard VPN Endpoints
3. Configure Standard VPN Groups
4. Assign Domains to Sites
5. Use Groups in Network Policy Rules

Understand Service and Data Center Groups

Prisma SD-WAN uses mapping of Standard VPN services and Prisma SD-WAN data centers to allow flexibility when creating network policy rules, while accounting for uniqueness across sites. For example, an administrator may want to create a single network policy that directs all HTTP and SSL Internet bound traffic through the closest Zscaler Enforcement Node (ZEN) in the region if it

is available and meets the application SLA, but if not, may leverage a Prisma SD-WAN Data Center site as a transit point.

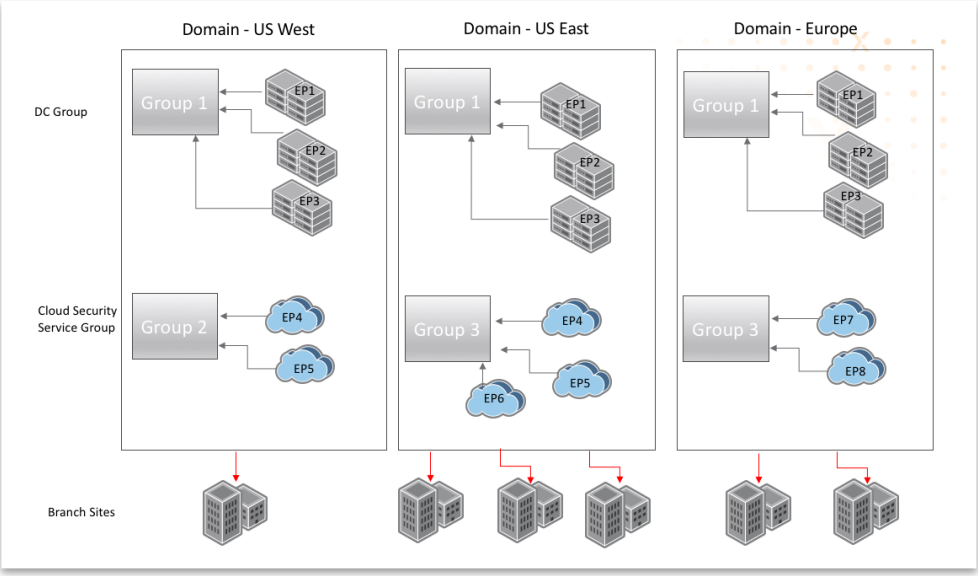
This is where the concept of endpoints, groups, and domains come into play. To leverage the underlying resources available to an administrator, it is important to understand how an endpoint, group, and domain work in the Prisma SD-WAN system.

Endpoint - A service **endpoint** is a label representing a specific location or network service. It can be of type Prisma SD-WAN, specifically Prisma SD-WAN Data Centers for Data Center transit services, or of type Standard VPN. In this release, the only Standard VPN service that can be configured VPNs to cloud security services. However, in a subsequent release, there could be other network services that would use this same construct.

Group - A service **group** is label representing a set of common service **endpoint** types**.** This service group label will be used in network policy rules to express intent to allow or force traffic to the defined service endpoint(s). It can be of type Prisma SD-WAN or Standard VPN and may contain zero or more service **endpoints**.

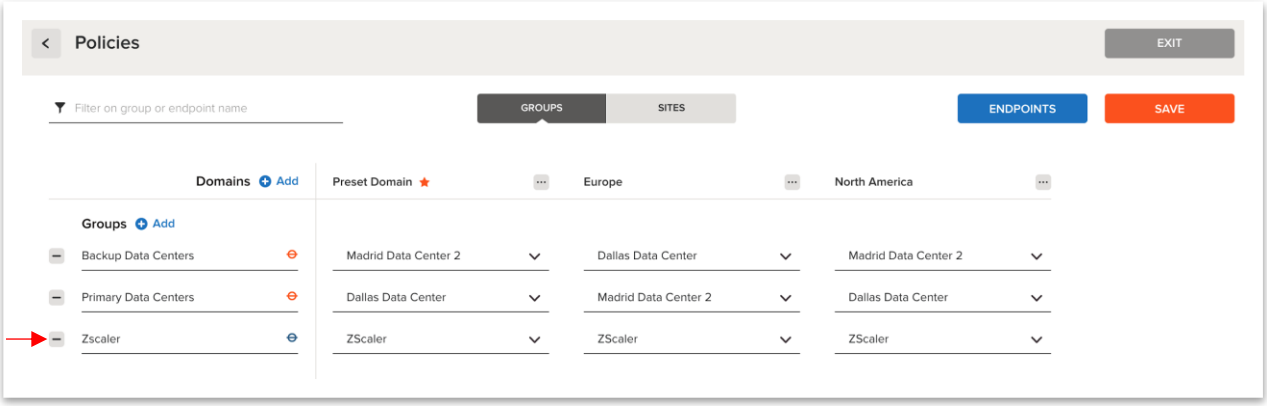
Domain - A **domain** is a collection of groups which can be assigned to a set of sites. There can be multiple domains defined, but a site may only be assigned to **one** domain at a time.

Note that a site will be able to use **only** the endpoints configured in a group within a domain that is assigned to the site. The same group, however, can be in multiple domains with different service endpoints, allowing you to use the same policy across different sites utilizing different endpoints.
Let us further explore the concept of endpoints, groups, and domains using the following illustration and screenshot.



The illustration displays how endpoints added to a group are associated with a domain. The domains are then bound to a site, thus mapping Standard VPN services or Prisma SD-WAN data centers uniquely for each site. Note that a group, with different endpoints, can be mapped to one or more domains and a domain can be mapped to one or more sites.

Another example to illustrate the concept is shown below as a screenshot. For a customer with sites in North America and Europe that has one Prisma SD-WAN-enabled data center in each region and has adopted Zscaler within each region the domain mapping is accomplished as follows:



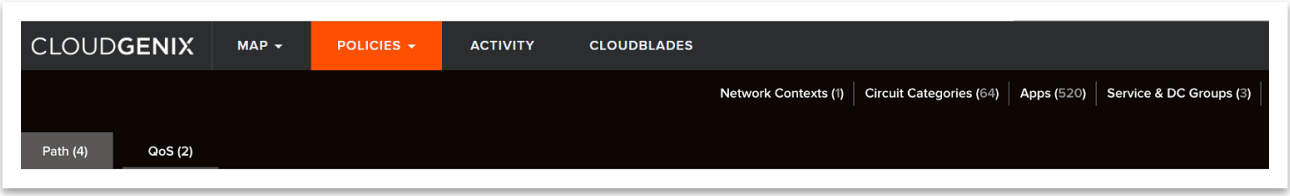
Note:

- The Zscaler CloudBlade creates a single group **Zscaler** with a single Standard VPN Endpoint.
- The Standard VPN endpoint has all possible Zscaler hostnames, and based on a latency check, the ION will build a VPN tunnel to the closest ZEN.
- The same endpoint can be added to more than one group.
- Only one active group and one backup group may be used in a network policy rule.

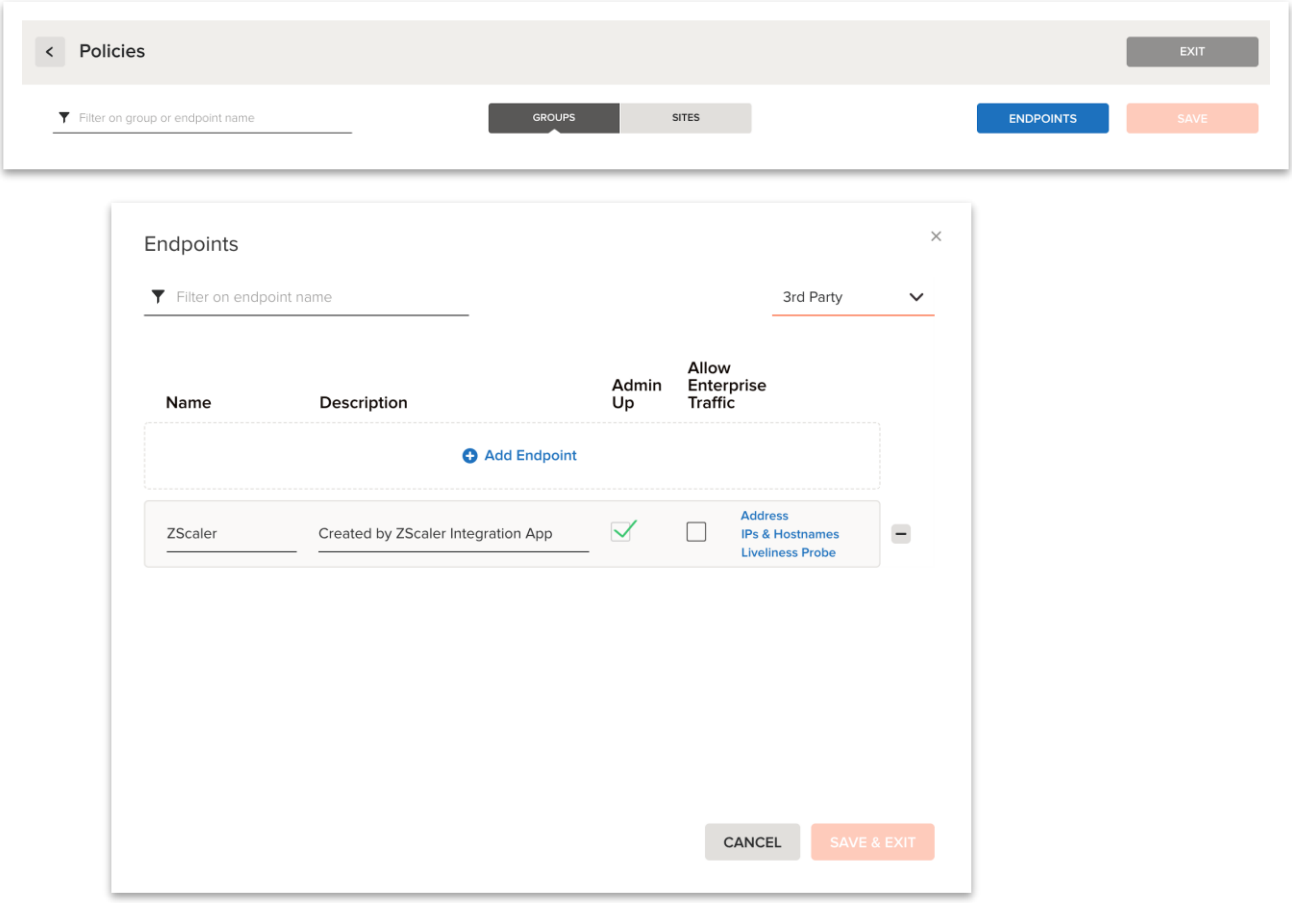
Verify Standard VPN Endpoints

With the Zscaler CloudBlade installed, a single Standard VPN endpoint with all ZEN hostnames will be created automatically. There is no action required, the steps below are provided only for reference.

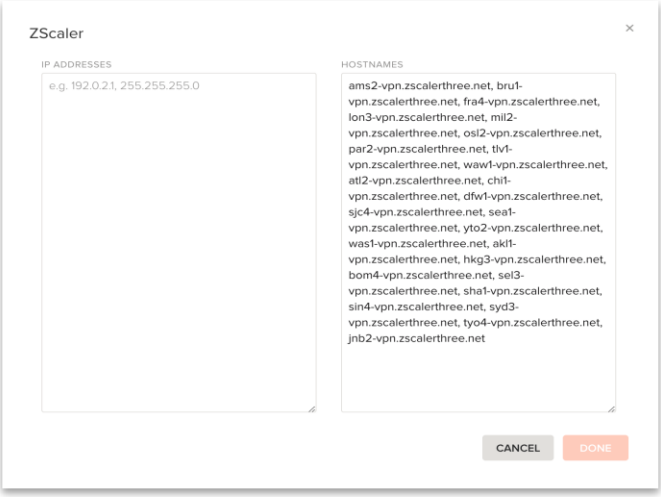
1. From the Prisma SD-WAN portal, click **Policies**, then **Stacked Policies**, and then select **Service & DC Groups**.



2. Select **Endpoints**, and filter by **Standard VPN**.

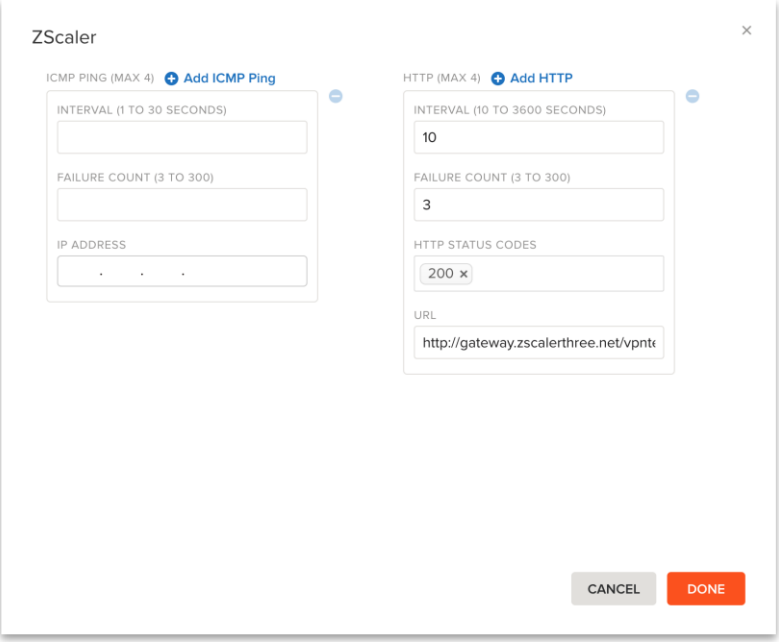


3. The host names programmed for this endpoint are displayed under the **Hostnames** tab.



The ION device assigned to sites and circuit types with the **AUTO-zscaler** tag will perform a latency check for each hostname listed under the Standard VPN endpoint. The list will be sorted based on the fastest to the slowest response. The first reachable hostname will be used to build the Standard VPN.

4. If the ZEN hostname selected becomes unavailable after the IPsec tunnel is established, either by IPsec DPD or via the Layer 7 health probe specified on the Standard VPN endpoint (see figure below), the ION device will attempt to establish a new IPsec VPN to the next hostname in the ordered list.



Since no action is required here, proceed to verifying **Groups** and **Domains**.

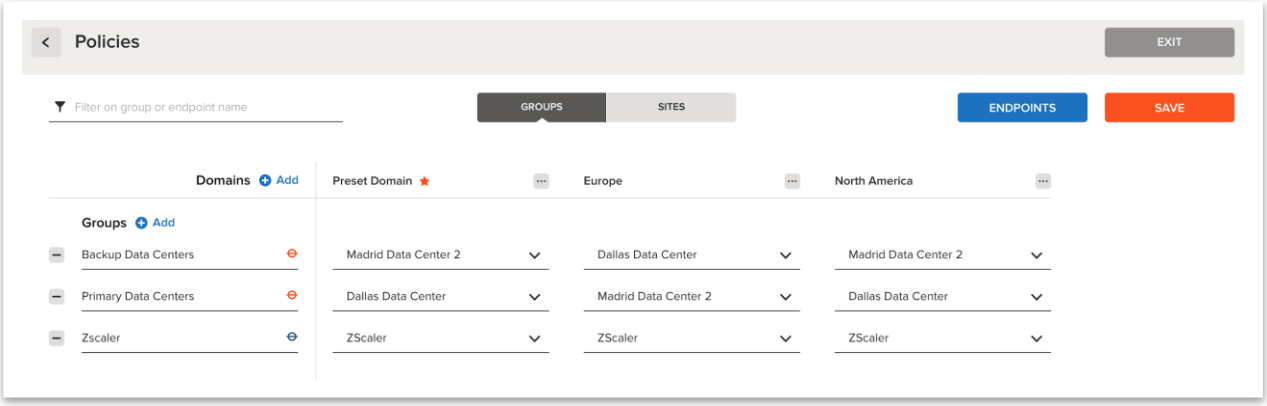
Verify Standard VPN Group

With the Zscaler CloudBlade installed, a Standard VPN group will automatically be created:

- **Zscaler**

There is no action required, as the domains associated with a site which has been tagged with **AUTO-zscaler** will automatically have the group and endpoint configured.

In the example below, the sites that are bound to the *Preset Domain*, *Europe*, and *North America* domains all must have one or more sites that were tagged with **AUTO-zscaler.**



Note: If more than one endpoint is a part of a group, all the endpoints will be considered equal in network policy path selection.

Finally, proceed to binding domains to sites.

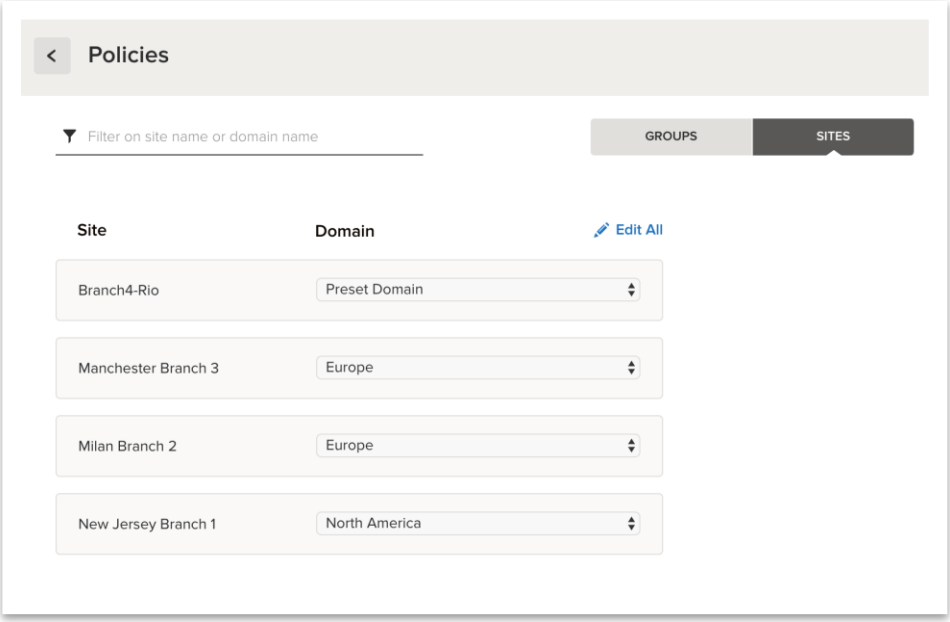
Assign Domains to Sites

Binding a domain is essentially mapping a site to a domain, enabling access to all the endpoints within groups/domain. Different domains can be mapped to different sites, but only one domain may be mapped per site. The workflow below is only for reference, since there are no configuration changes required for the Zscaler CloudBlade.

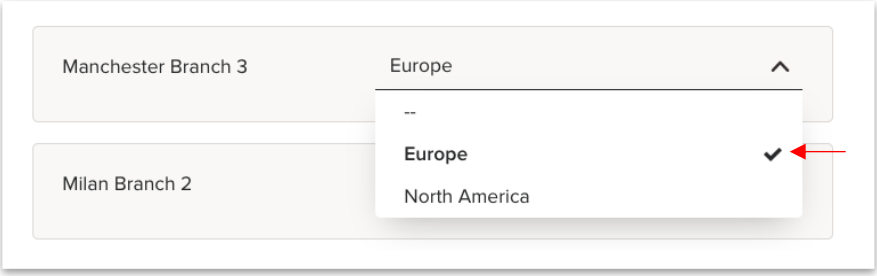
To bind a domain to a site:

1. Click **Policies**, select **Network Policies (Original)** or **Stacked Policies**, and then select **Service & DC Groups**.

2. Select **Sites.**



3. From the **Domain** drop-down list next to each site, select the appropriate domain. To edit information for all sites at a time, select the **Edit All** button.



4. Finally, click **Save**.

Use Groups in Network Policy Rules

Before you can use a Standard VPN in a policy rule, you need to define service endpoint groups. Each group can have one or more Prisma SD-WAN data centers or Standard VPN service endpoints. A group will be used in policy rules. The domain defining the mappings for endpoints to groups must be assigned to a site for the policy rules using the group to be effective. For more information, refer to *Managing Services and Data Center Groups*.

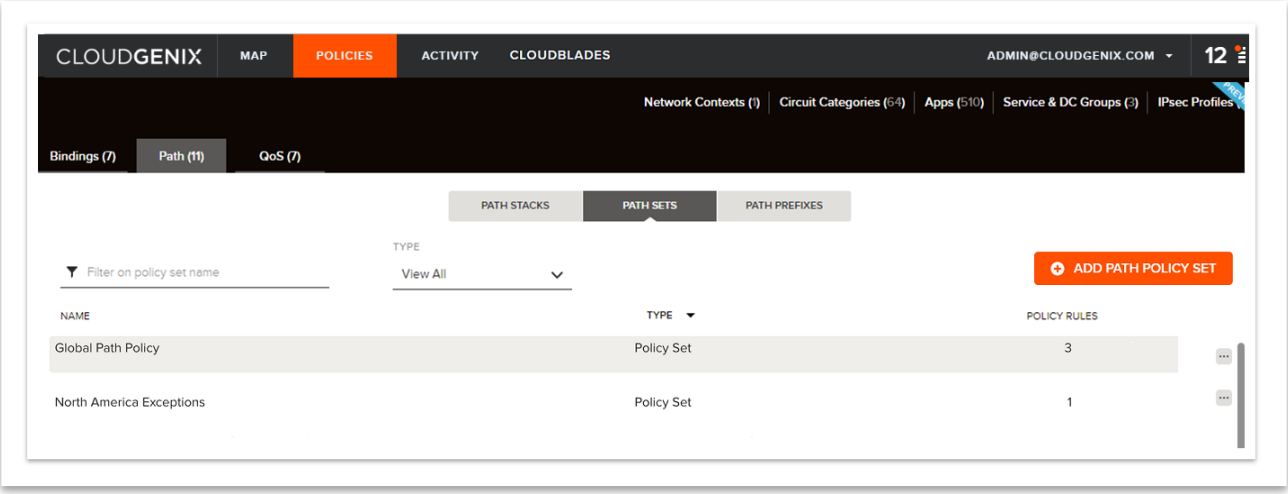
There can be four combinations of Active/Backup groups that can be used in Policies. You may select just one **Prisma SD-WAN group** or one **non-Prisma SD-WAN group** as an active or backup path in policies. For example:

Active Group	Backup Group	Example
Standard VPN	**Prisma SD-WAN**	Internet-bound SSL traffic from a branch site will transit through the Cloud Security Service. In the event all Standard VPN paths to any of the endpoints in the Primary Cloud Security Service group are not available, internet-bound SSL traffic will transit through one of the Prisma SD-WAN data center endpoints assigned to that via the Prisma SD-WAN VPN.
Prisma SD-WAI	**Standard VPN**	Internet-bound SSL traffic from a branch site will transit through one of the Prisma SD-WAN data center endpoints assigned to that group via the Prisma SD-VPNs. In the event all Prisma SD-WAN VPNs to all of the Data Center endpoints in group are unavailable, internet-bound SSL traffic will transit through the Cloud Security Service via one of the Standard VPN paths to any of the endpoints in the Standard VPN group.
Standard VPN	**Standard VPN**	Internet-bound SSL traffic from a branch site will transit through the primary cloud security service via one of the Standard VPN paths to any of the endpoints in the primary cloud security service group. In the event all Standard VPNs are down to all endpoints in the primary group, the Internet bound SSL traffic will transit through the backup cloud security service via one of the Standard VPN paths to the endpoints that are part of the backup group.
Prisma SD-WAN	**Prisma SD-WAN**	Internet-bound SSL traffic from a branch site will transit through one of the Prisma SD-WAN data center endpoints assigned to the active group via the VPNs. In the event all Prisma SD-WAN VPNs to all of those endpoints are down, internet-bound SSL traffic will transit through one of the Prisma SD-WAN data center endpoints assigned to the backup group via the Prisma SD-WAN VPNs.

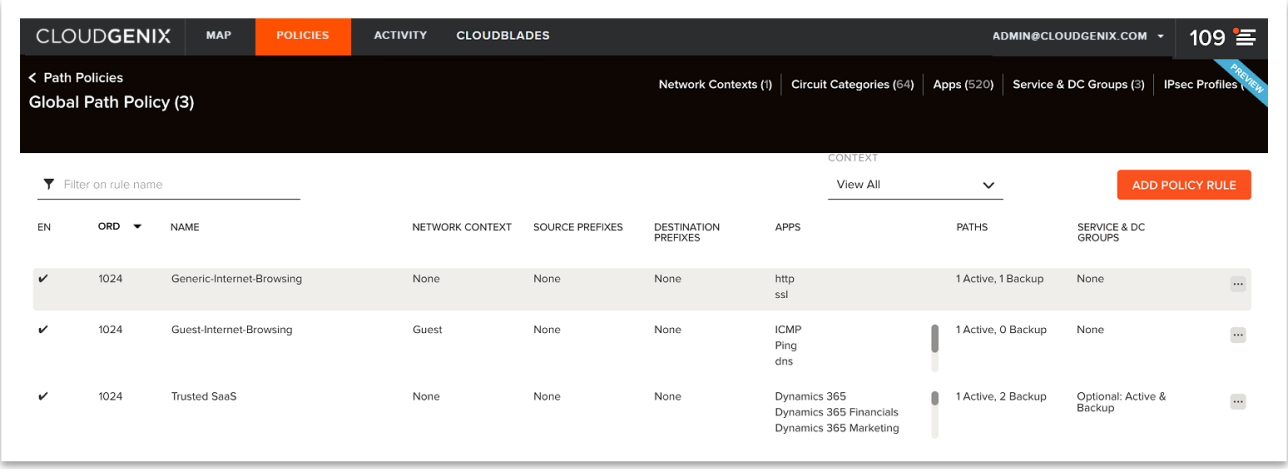
Use a Group in Stacked Policies

To use a group in **Stacked Policies**:

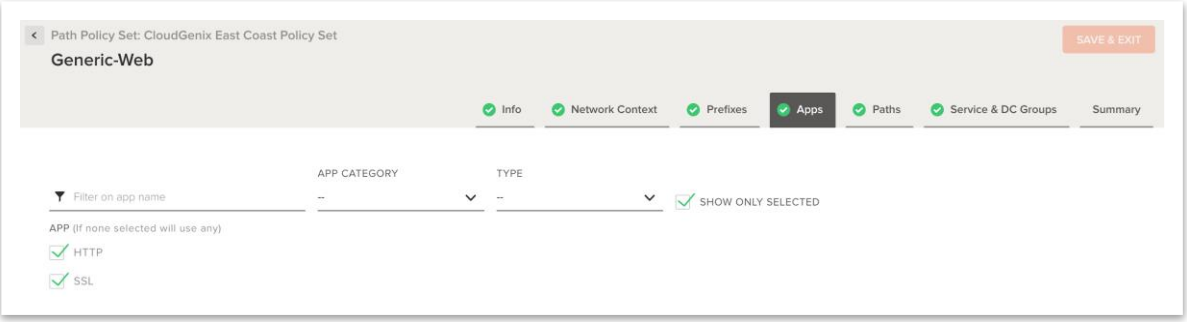
1. From **Policies**, select **Stacked Policies**, select **Path Sets**, and then select a path policy set.



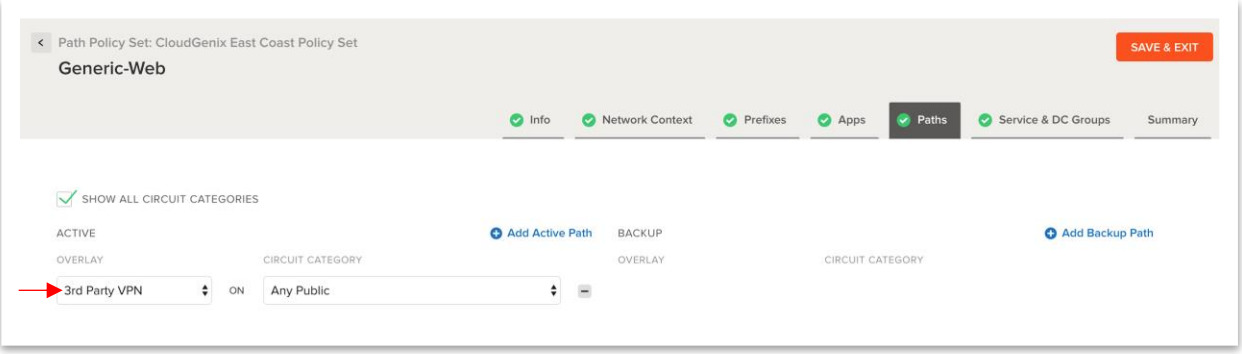
2. Within the policy set, select a rule to edit or add a new rule.



3. Select the required applications or confirm that the required applications are selected.

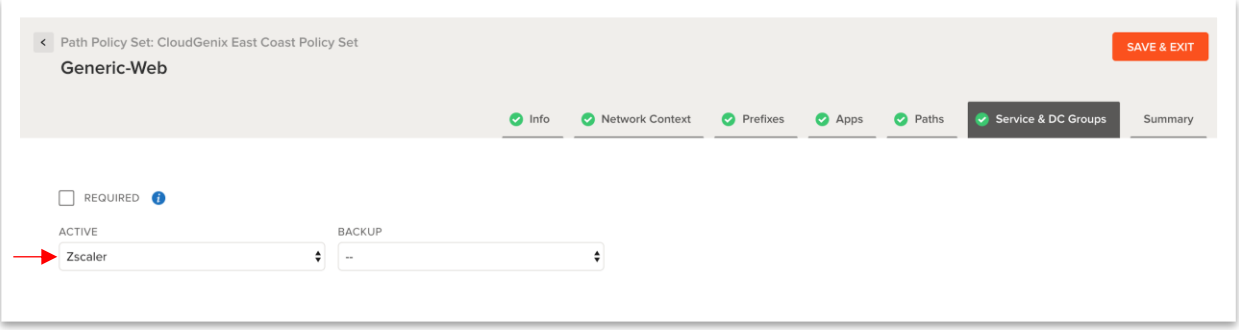


4. On the **Paths** tab, select the **Active** and/or **Backup** path as **Standard VPN** on **<circuit category>** or **Any Public / Private** to allow the system to use any/ all paths of that type.



Note: You can mix Standard VPNs with other available paths – private, public, direct or VPNs.

5. On the **Service & DC Group** tab, select **Zscaler** as the Standard VPN group, and click **Save & Exit**.



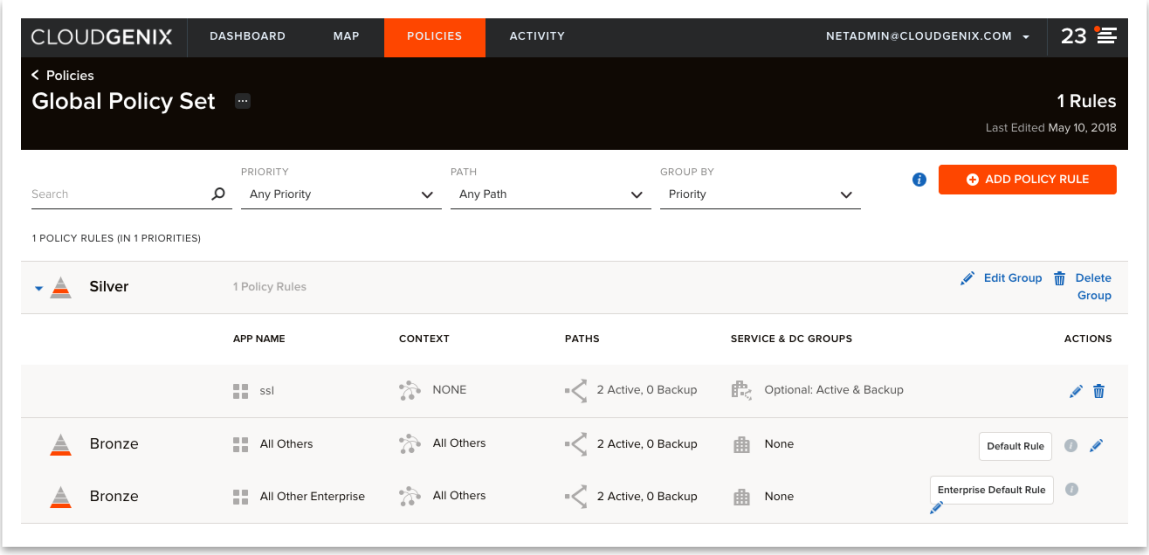
Note:

- If **Standard VPN** path is used in a network policy, then you must have a Standard VPN Services and DC Group defined in the policy for the traffic to transit through that group. If not, traffic will be black-holed.
- If **Required** is selected, traffic will always transit through the Services and DC Group. If not selected, traffic may or may not transit through the Services and DC Group per policy.

Use a Group in Network policies (Original)

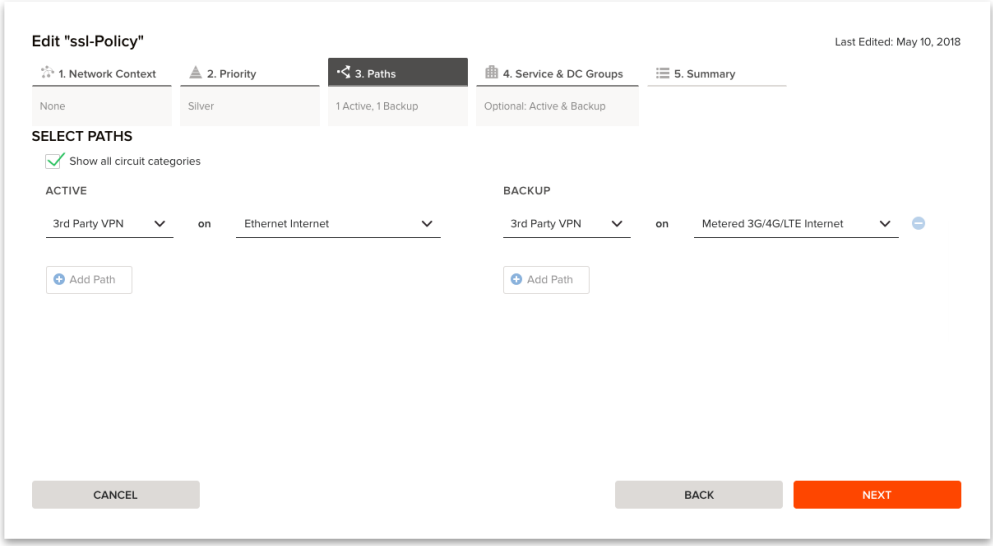
To use a group in **Network Polices (Original)**:

1. From **Policies,** select **Network Policies (Original)**, select an application and click the icon next to it. Alternatively, you may select **Edit Group** to edit priority and path for all the applications within that group.



2. On the **Paths** tab, select **Standard VPN** either for an **Active** path or a **Backup** path.

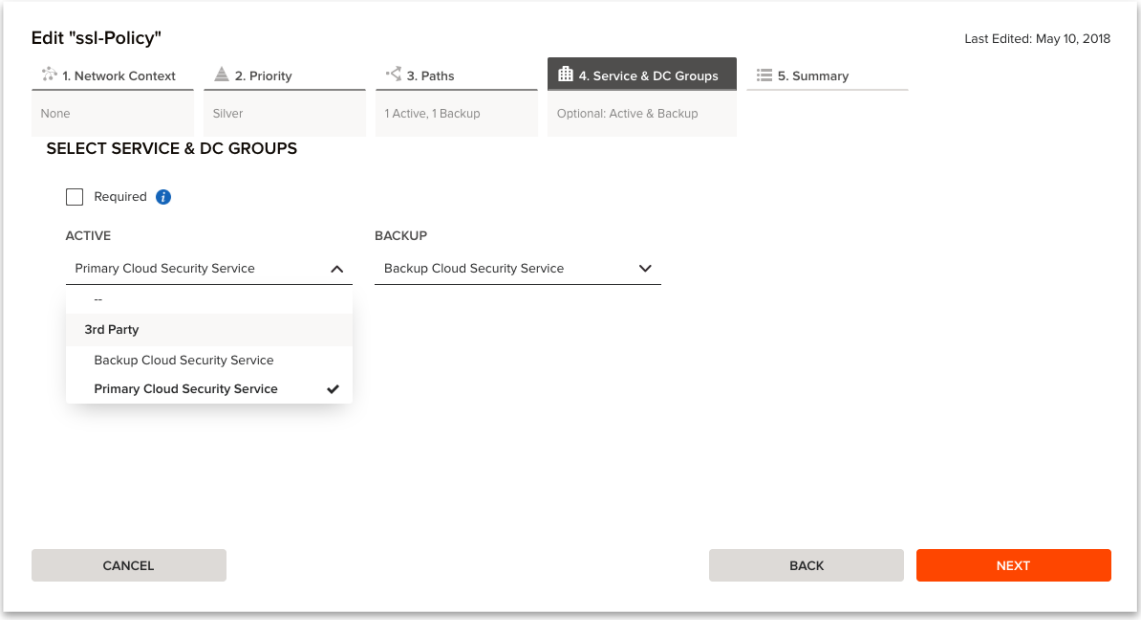
Note: You can mix Standard VPNs with other available paths – private, public, direct or VPNs.



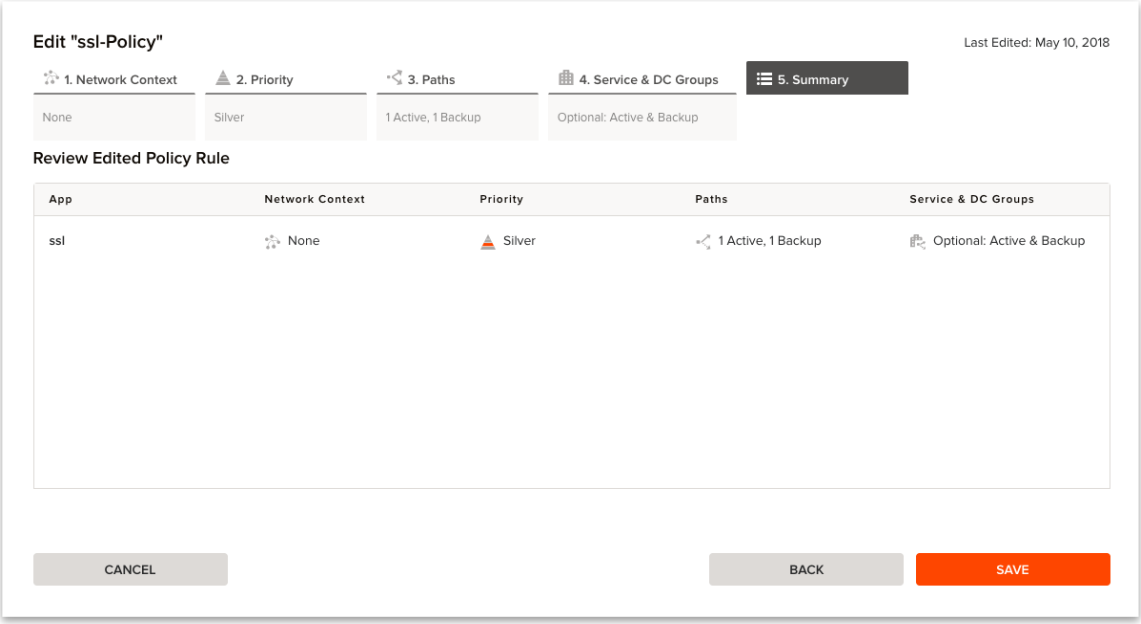
3. Click **Next** to navigate to the **Services and DC Group** tab. Choose a group from either the **Active** or **Backup** drop-down lists.

Note:

- If **Standard VPN** path is used in a network policy, then you must have a Standard VPN Services and DC Group defined in the policy for the traffic to transit through that group. If not, traffic will be black-holed.
- If **Required** is selected, traffic will always transit through the Services and DC Group. If not selected, traffic may or may not transit through the Services and DC Group per policy.



4. Check the summary, and then click **Save** to save the policy rule.


Edit "ssl-Policy"
Last Edited: May 10, 2018
1. Network Context
2. Priority
3. Paths
4. Service & DC Groups
5. Summary
None
Silver
1 Active, 1 Backup
Optional: Active & Backup
Review Edited Policy Rule
App
Network Context
Priority
Paths
Service & DC Groups
ssl
None
Silver
1 Active, 1 Backup
Optional: Active & Backup
CANCEL
BACK
SAVE

Managing and Troubleshooting the Zscaler CloudBlade

The following sections detail various operations and troubleshooting scenarios related to the integration process.

Enabling, Pausing, Disabling and Uninstalling the CloudBlade.

After the CloudBlade is set up, operations can be done using the CloudBlade panel. These operations have various effects on the tunnels and configurations in Prisma SD-WAN and Zscaler.

- Set the CloudBlade to **Enabled**
  Enabled is the standard expected mode of operation for the CloudBlade. The CloudBlade will run every 60 seconds, find any new Sites/Circuits with the appropriate tags, and configure the integration on Zscaler and Prisma SD-WAN. In addition, during this integration run, if any settings were previously modified manually on either Prisma SD-WAN or Zscaler (e.g. VPN credentials changed, or Location deleted in Zscaler), these will be reverted to the known good state automatically.

- Set the CloudBlade to **Paused**
  Pausing the CloudBlade stops all future integration runs, but leaves any created objects intact. This stops any future objects from getting created but does **NOT** prevent removal of any unconfigured/untagged objects on either Prisma SD-WAN or Zscaler.

- Set the CloudBlade to **Disabled**
  Disabling the CloudBlade tells the system to **remove and delete all configurations** created by the CloudBlade. This can cause communication interruptions if policy is not set to use other paths. Note that IPsec policies, IKE policies, and Prisma SD-WAN Endpoints and Service and DC groups are not automatically deleted and must be removed manually.

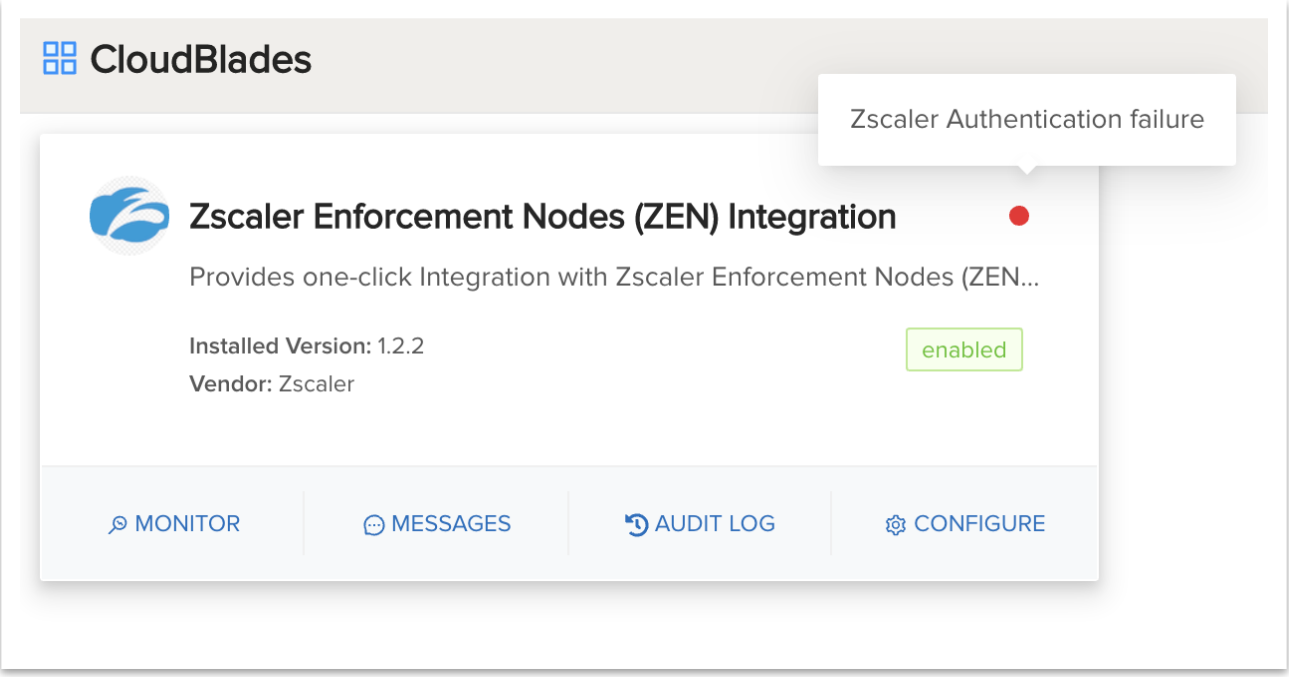
- **Uninstalling** the CloudBlade
  Uninstalling the CloudBlade removes the configuration for the CloudBlade, and immediately stops any changes by the CloudBlade. Uninstalling the CloudBlade does not automatically remove configuration from all sites and objects. The CloudBlade may be uninstalled and reinstalled to facilitate upgrades or downgrades to different versions without traffic interruption. To completely remove all items, please set the CloudBlade to **Disabled** for 2-3 Integration Run periods (180 seconds) before uninstalling the CloudBlade.

Installation Troubleshooting

A few common scenarios administrators should be aware of when attempting to do the initial installation of the Zscaler CloudBlade.

Wrong API Key or Partner Admin credentials

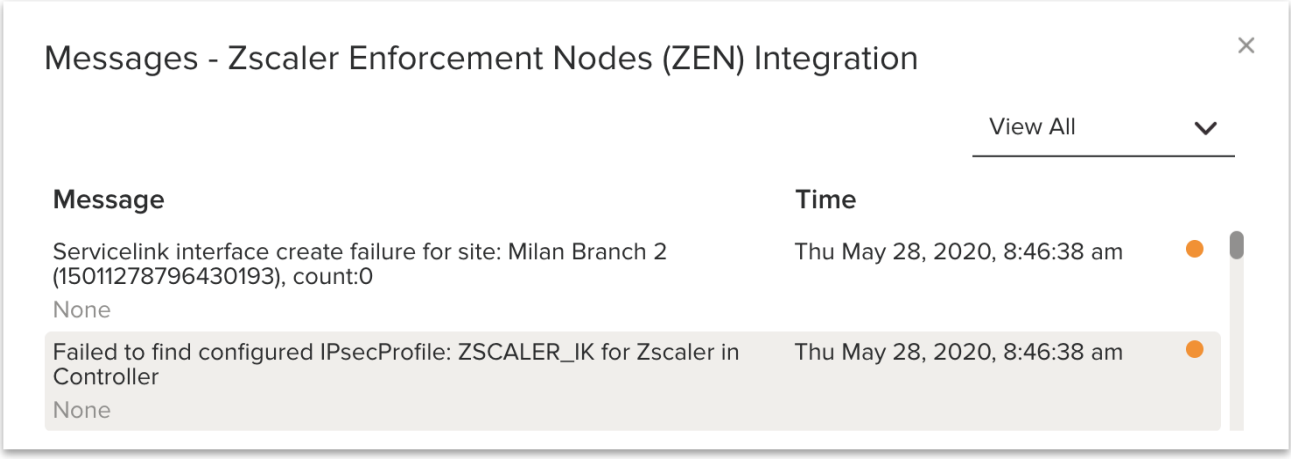
If an administrator incorrectly enters the API key or Partner Admin credentials, the system will alert the administrator by reporting the status on the **CloudBlade** page.



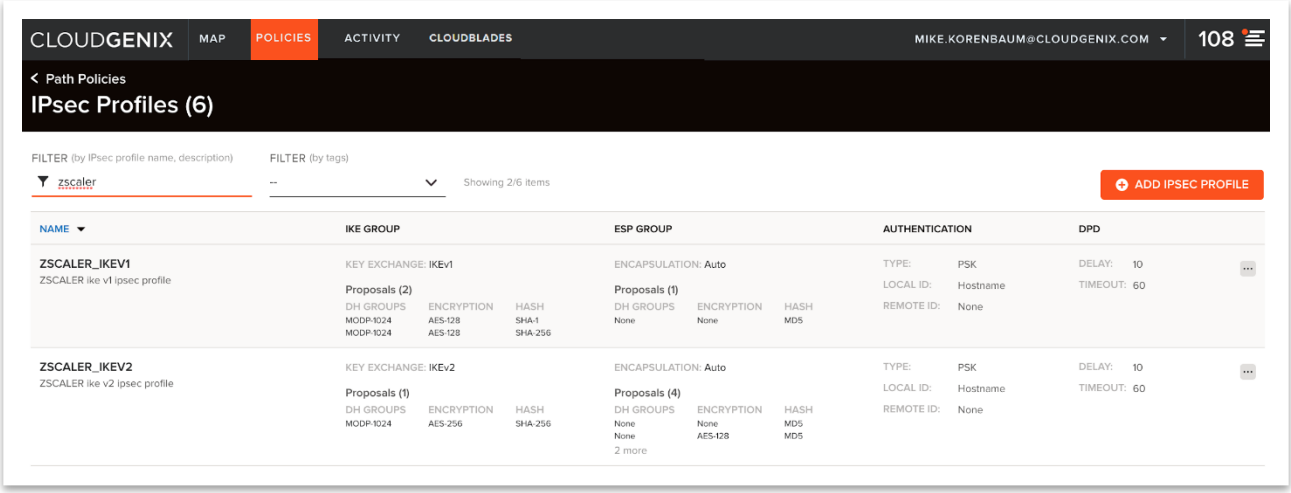
Prisma SD-WAN Standard VPNs not created

There could be a scenario in which all user credentials, keys, and tokens are correct, and the Zscaler Location and VPN credential objects are also created. However, the Prisma SD-WAN VPNs are not created. This can be due to the pre-built IPsec profiles based on Zscaler's recommended best practices, which have not been allocated to your Prisma SD-WAN tenant. Another reason could be that the custom IPsec profile name specified in your CloudBlade configuration does not exist (or has a typo in it).

This condition can be validated by selecting the **Messages** link on the CloudBlade card and looking for an error message similar to the one below.



To verify that these IPsec profiles exist, navigate to **Stacked Policies** > **IPsec Profiles**, and check if the profiles shown in the example below are displayed. If these two profiles are not present, please contact Prisma SD-WAN support. Or, create your own IPsec profile and that name in your CloudBlade configuration.



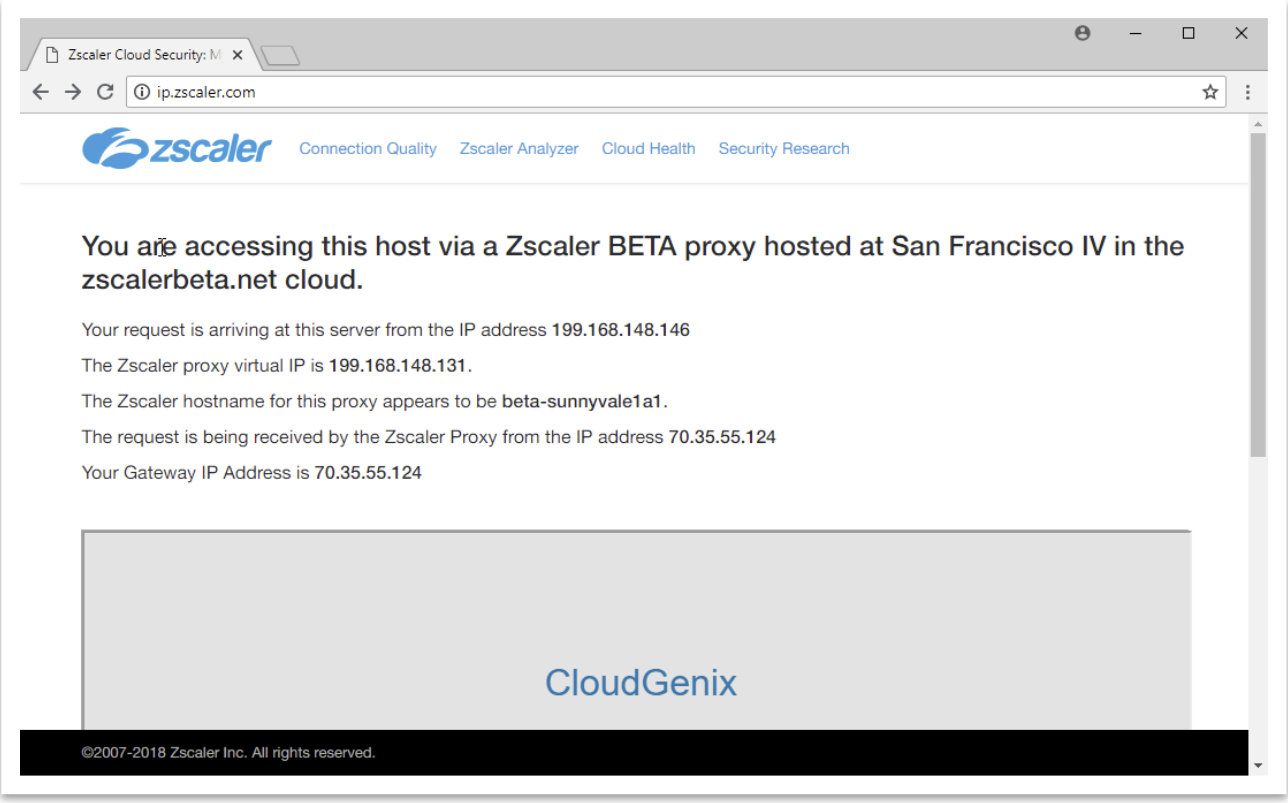
The next section will cover troubleshooting issues once the CloudBlade is installed.

Troubleshooting Standard VPNs

Start with the **Zscaler Test Page** to verify and troubleshoot client traffic to and through Zscaler Enforcement Nodes (ZENs). All application and path metrics will also be collected and reported, and all application monitoring alarms and alerts will be generated for Standard VPNs. To troubleshoot Standard VPNs, view **Alerts and Alarms, Connectivity of Standard VPNs** at the site level, and **Activity** charts to view possible issues with the VPN. In addition, device toolkit commands can be used to view Standard VPN **stats**, **status**, and **summary**.

Use the Zscaler Test Page

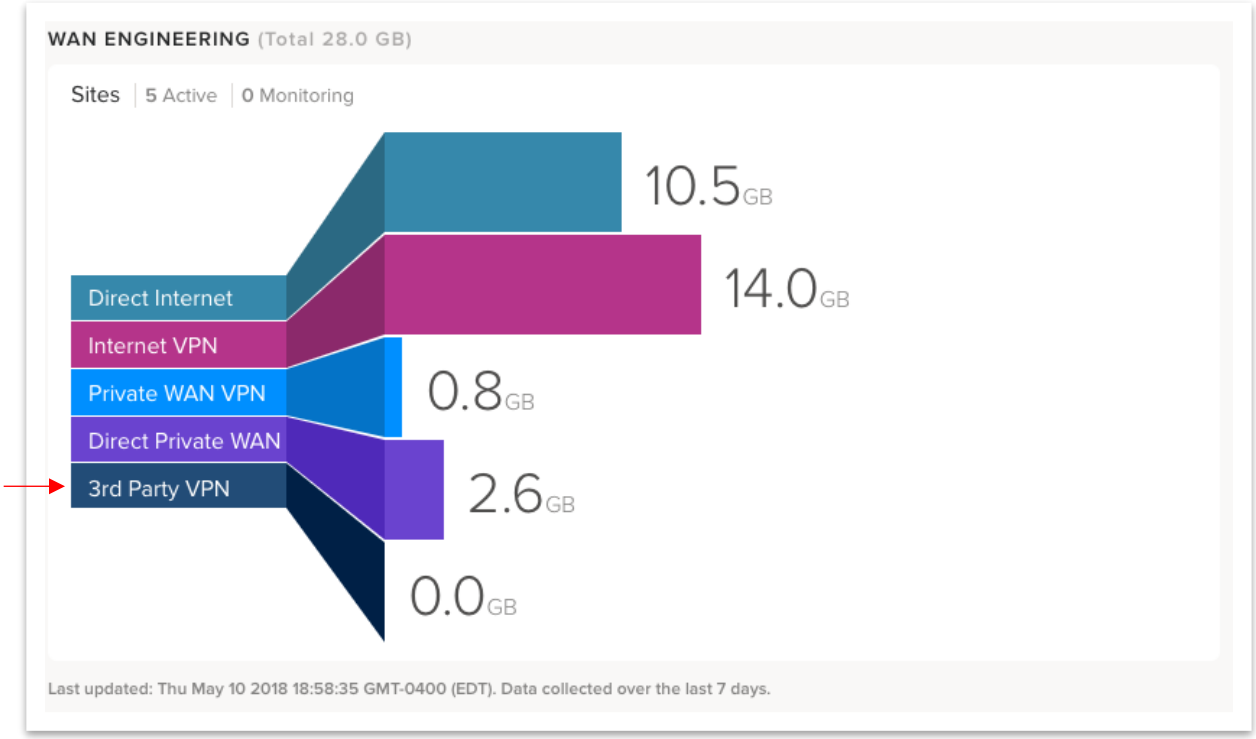
Zscaler provides a diagnostic page that allows for verification and troubleshooting of client traffic to and through Zscaler ZENs. To access the page from any client, open the link http://ip.zscaler.com.



For more details on this tool, refer to the Zscaler Knowledgebase article, 'How can I check if a user's traffic is going to Zscaler?"'

View Standard VPN on the Dashboard

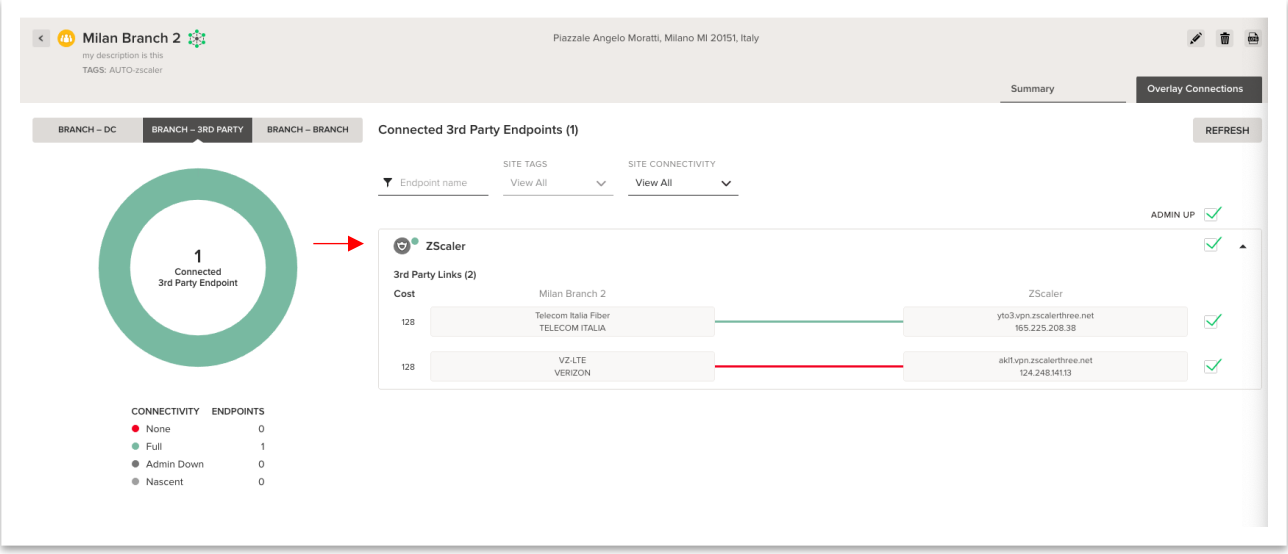
In addition to direct and VPN internet and private WAN paths, the **Prisma SD-WAN Dashboard** will now display traffic on the **Standard VPN link**.



View Standard VPN at Site Level

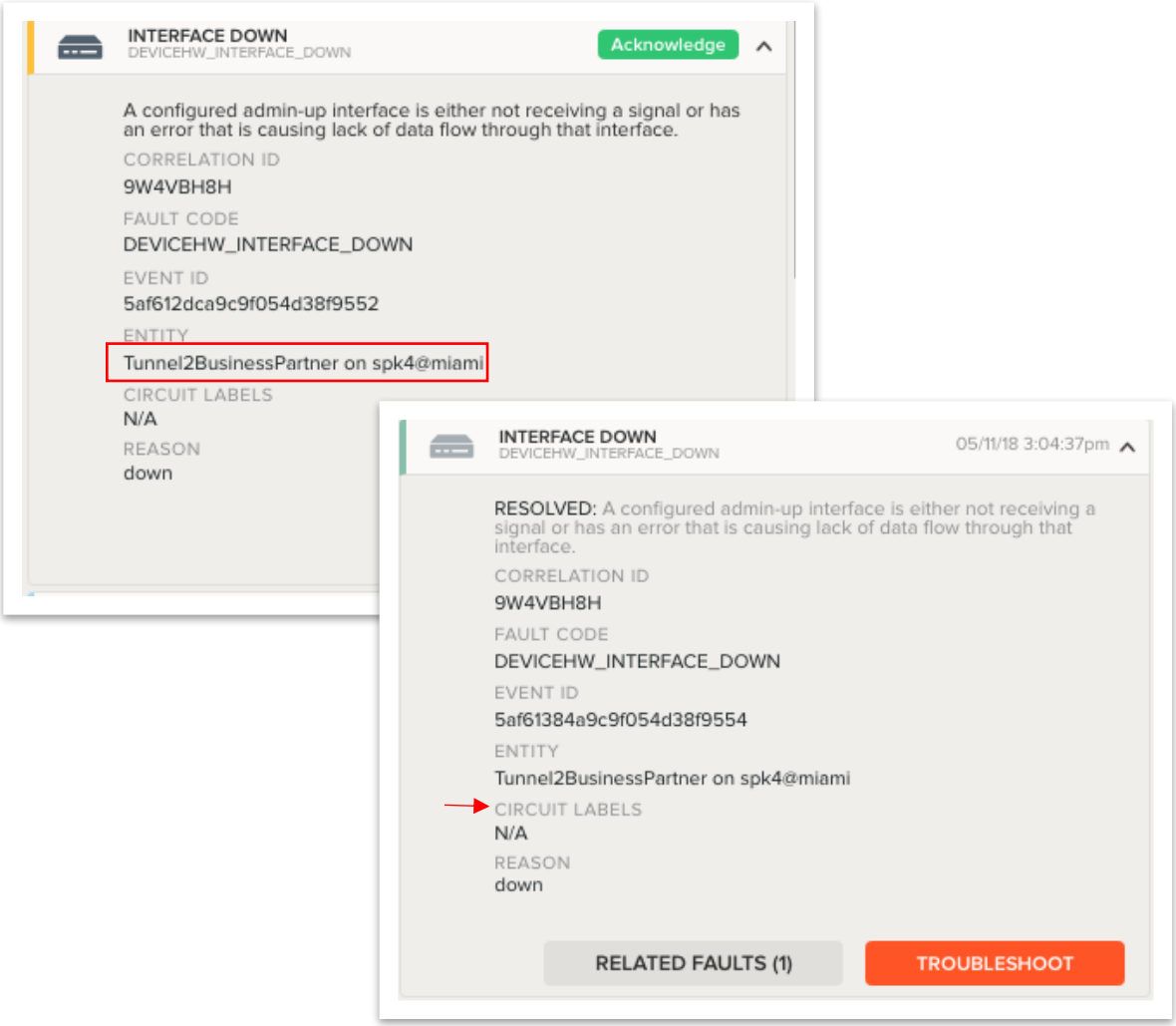
The **Map** will provide a quick view of interface status at the site level.

Select **MAP,** select a **site**, and under **Connectivity**, click **Standard VPN** to view the status of the Standard VPN.



View Alerts and Alarms

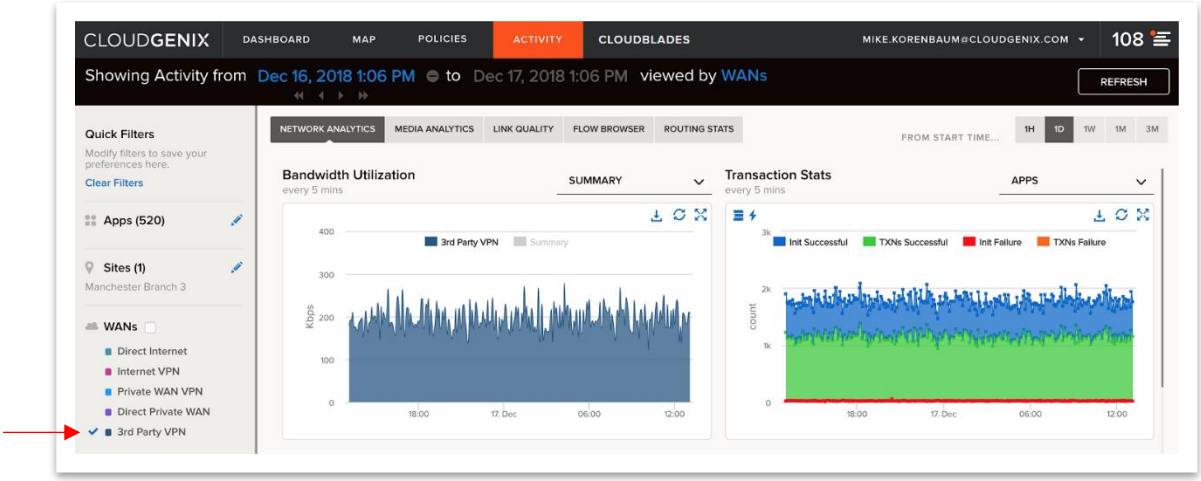
If a Standard VPN tunnel interface is down, an alarm will be raised, just like it would for any other interface within the system.

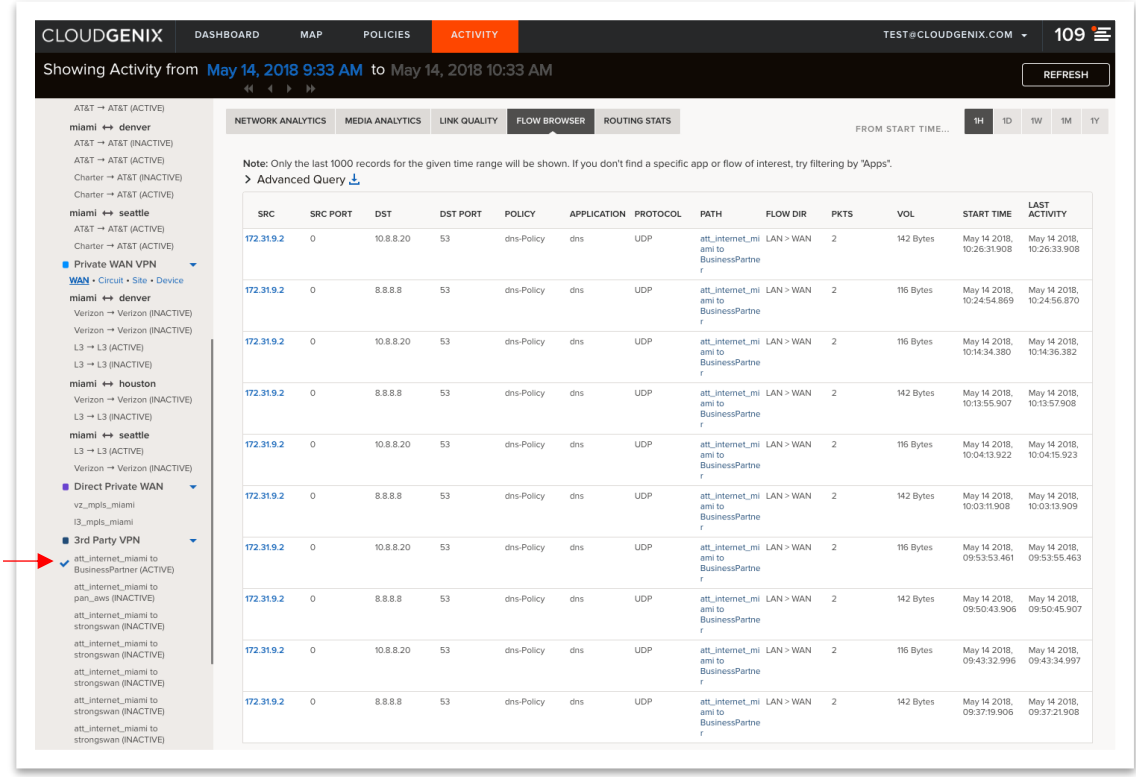


View Activity Charts

Activity Charts can be filtered based on paths, including Standard VPNs. Traffic analytics can be viewed through Network Analytics, Media Analytics, and Flow Browser Charts for Standard VPNs.

From **Quick Filters**, under **WANs**, make sure to select **Standard VPN**. Or, from **Paths**, select a specific Standard VPN to display analytics for that path.





Use the Device Toolkit

The following device toolkit commands will provide Standard VPN status and statistics.

dump servicelink summary

```
Branch ION 3000# dump servicelink summary
------------- SERVICE LINKS ---------------------------------
Total      : 1
TotalUP    : 1
TotalDown  : 0
-------------------------------------------------------------
SlDev       SlName                              Status ParentDev LocalIP              Peer                 IpsecProfile
-------------------------------------------------------------
sl8         sl-zscaler-15132962570970071        up     eth2      70.35.55.124         104.129.202.10      ZSCALER_IKEV1
```

dump servicelink stats

```
Branch ION 3000# dump servicelink stats slname=sl-zscaler-15132962570970071

No of times IkeRekeyed     : 0
No of times ChildRekeyed   : 1
No of times HoldDown       : 0
No of times TunnelUp       : 2
No of times TunnelDown     : 1
No of Incoming Bytes      : 704132205
No of Outgoing  Bytes      : 64453909
No of Incoming Packets    : 879522
No of Outgoing  Packets    : 865419
```

dump servicelink status

```
Branch ION 3000# dump servicelink status slname=sl-zscaler-15132962570970071

ServiceLink : sl8
IkeSa:
   Version         :1
   State           :Up
   Local IP        :70.35.55.124
   Local ID        :15451095560390112@demo-cloudgenix.com
   Remote IP       :104.129.202.10
   Remote ID       :104.129.202.10
   Encryption Algo :AES_CBC_128
   Integrity Algo  :HMAC_SHA1_96
   Rekey Time      :2018-12-19 11:35:32.572152899 +0000 UTC (52971s)
   Dhgroup         :MODP_1024
ChildSa:
   SPI In          :977a8bf8
   SPI Out         :06d97102
   Encryption Algo :NULL_
   Integrity Algo  :HMAC_MD5_96
   Dhgroup         :
   Rekey Time      :2018-12-19 03:30:22.572235909 +0000 UTC (23861s)
   Life Time       :2018-12-19 03:54:50.572246359 +0000 UTC (25329s)
   Install Time    :2018-12-18 19:54:50.572256139 +0000 UTC (3471s)

Peer configured on service endpoint
   Service endpoint name: ZScaler
   Order of connection Try:
      Ipv4Addr: 104.129.202.10       HostName: sjc4-vpn.zscalerthree.net
      Ipv4Addr: 165.225.50.22        HostName: sea1-vpn.zscalerthree.net
      Ipv4Addr: 165.225.34.44        HostName: dfw1-vpn.zscalerthree.net
      Ipv4Addr: 165.225.0.165        HostName: chi1-vpn.zscalerthree.net
      Ipv4Addr: 104.129.206.161      HostName: atl2-vpn.zscalerthree.net
```

```
     Ipv4Addr: 165.225.36.39        HostName: yto2-vpn.zscalerthree.net
     Ipv4Addr: 165.225.48.10        HostName: was1-vpn.zscalerthree.net
     Ipv4Addr: 165.225.110.24       HostName: tyo4-vpn.zscalerthree.net
     Ipv4Addr: 165.225.16.38        HostName: lon3-vpn.zscalerthree.net
     Ipv4Addr: 124.248.141.13       HostName: akl1-vpn.zscalerthree.net
     Ipv4Addr: 165.225.88.39        HostName: bru1-vpn.zscalerthree.net
     Ipv4Addr: 1.234.57.13          HostName: sel3-vpn.zscalerthree.net
     Ipv4Addr: 165.225.76.42        HostName: par2-vpn.zscalerthree.net
     Ipv4Addr: 165.225.28.14        HostName: ams2-vpn.zscalerthree.net
     Ipv4Addr: 165.225.24.10        HostName: fra4-vpn.zscalerthree.net
     Ipv4Addr: 165.225.116.24       HostName: hkg3-vpn.zscalerthree.net
     Ipv4Addr: 165.225.86.39        HostName: mil2-vpn.zscalerthree.net
     Ipv4Addr: 213.52.102.19        HostName: osl2-vpn.zscalerthree.net
     Ipv4Addr: 165.225.84.39        HostName: waw1-vpn.zscalerthree.net
     Ipv4Addr: 165.225.112.24       HostName: sin4-vpn.zscalerthree.net
     Ipv4Addr: 165.225.114.24       HostName: syd3-vpn.zscalerthree.net
     Ipv4Addr: 58.220.95.19         HostName: sha1-vpn.zscalerthree.net
     Ipv4Addr: 94.188.131.35        HostName: tlv1-vpn.zscalerthree.net
     Ipv4Addr: 165.225.106.39       HostName: bom4-vpn.zscalerthree.net
     Ipv4Addr: 197.98.201.17        HostName: jnb2-vpn.zscalerthree.net
```

dump servicelink endpoints

```
Branch ION 3000# dump serviceendpoints all
-----------------------------------------------------------------------------------------------
Name                                Type               AdminUp      AllowEnterpriseTraffic
-----------------------------------------------------------------------------------------------
SC us-east-1                        cg-transit           true      false
ZScaler                             non-cg-transit       true      false
Branch ION 3000# dump serviceendpoints endpoint=ZScaler
Name                          : ZScaler
Type                          : non-cg-transit
AdminUp                       : true
AllowEnterpriseTraffic        : false
LivelinessProbe:
          HTTP LivelinessProbe
          -----------------------------------------
          URL                 : http://gateway.zscalerthree.net/vpntest
          Interval  : 10
          FailureCount        : 3
          HttpStatusCodes     : 200
          -----------------------------------------
ServiceLinkPeer:
          Hostnames:
           ams2-vpn.zscalerthree.net
           bru1-vpn.zscalerthree.net
           fra4-vpn.zscalerthree.net
           lon3-vpn.zscalerthree.net
           mil2-vpn.zscalerthree.net
           osl2-vpn.zscalerthree.net
           par2-vpn.zscalerthree.net
           tlv1-vpn.zscalerthree.net
           waw1-vpn.zscalerthree.net
           atl2-vpn.zscalerthree.net
           chi1-vpn.zscalerthree.net
           dfw1-vpn.zscalerthree.net
           sjc4-vpn.zscalerthree.net
           sea1-vpn.zscalerthree.net
           yto2-vpn.zscalerthree.net
           was1-vpn.zscalerthree.net
           akl1-vpn.zscalerthree.net
           hkg3-vpn.zscalerthree.net
           bom4-vpn.zscalerthree.net
           sel3-vpn.zscalerthree.net
           sha1-vpn.zscalerthree.net
           sin4-vpn.zscalerthree.net
           syd3-vpn.zscalerthree.net
           tyo4-vpn.zscalerthree.net
           jnb2-vpn.zscalerthree.net
```

For more information on device toolkit commands, refer to the *Prisma SD-WAN Device Toolkit Reference Guide*.

Appendix A: Zscaler Location Gateway Options

CloudBlade version 1.2.2 supports the following gateway options:

Options	Corresponding Prisma Access for Networks Tag
Use XFF from Client Request	**Gateway Options**: <True | False> **Sub Locations**: Disabled
Enforce Zscaler App SSL Setting	Deprecated
Enable SSL Inspection	Deprecated
Enforce Firewall Control	<True | False>
Enforce Authentication	<True | False>
Enable IP Surrogate	<True | False> **Idle time: <val>** **Idle time metric: <minutes | hours | days>**
Enable Surrogate IP for Known Browsers	<True | False> **Refresh time: <val>** **Refresh time metric: <minutes | hours | days>**

Enable Caution	**<True | False>**
Enable AUP	**<True | False>** **Frequency (days): <val>** **Block Internet Access: <True | False>** **Force SSL Inspection: <True False>**

For more information on Zscaler gateway options, refer to https://help.zscaler.com/zia/configuring-locations